Symantec AntiVirus™ Scan Engine Implementation Guide

Symantec AntiVirus™ Scan Engine Implementation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 4.0 12/2002 Inline

Copyright Notice

Copyright © 2000-2002 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. CarrierScan Server, Bloodhound, LiveUpdate, NAVEX, Symantec AntiVirus, and Symantec Security Response are trademarks of Symantec Corporation. Sun, Sun Microsystems, the Sun logo, Sun Enterprise, Java, Ultra, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc., in the United States and other countries. SPARC is a registered trademark of SPARC International, Inc. Products bearing SPARC trademarks are based on an architecture developed by Sun Microsystems, Inc. Microsoft, ActiveX, Windows, Windows NT, and the Windows Logo are registered trademarks of Microsoft Corporation in the United States and other countries. Intel and Pentium are registered trademarks of Intel Corporation. Red Hat is a registered trademark of Red Hat Software, Inc., in the United States and other countries. Linux is a registered trademark of Linus Torvalds. NetApp, Data ONTAP, NetCache, Network Appliance, and Web Filer are registered trademarks or trademarks of Network Appliance, Inc., in the United States and other countries. Adobe, Acrobat, and Acrobat Reader are trademarks of Adobe Systems Incorporated. THIS PRODUCT IS NOT ENDORSED OR SPONSORED BY ADOBE SYSTEMS INCORPORATED, PUBLISHERS OF ADOBE ACROBAT.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

A modified version of a freeware SNMP library is used in this software. This software is Copyright © 1988, 1989 by Carnegie Mellon University All Rights Reserved. Permission to

use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

CMU software disclaimer: “CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.”

A set of Unicode handling libraries is used in this software. This software is Copyright (c) 1995-2002 International Business Machines Corporation and others. All rights reserved. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation. Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

IBM software disclaimer: “THE SOFTWARE IS PROVIDED ‘AS IS’, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.”

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

SYMANTEC SOFTWARE LICENSE AGREEMENT
ENTERPRISE ANTIVIRUS SOFTWARE

THIS LICENSE AGREEMENT SUPERSEDES THE LICENSE AGREEMENT CONTAINED IN THE SOFTWARE INSTALLATION AND DOCUMENTATION.

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE" OR "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. LICENSE:

The software and documentation that accompanies this license (collectively the "Software") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the quantity of the Software for which You have paid the applicable license fees after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, Your rights and obligations with respect to the use of licensed copies of this Software are as follows:

YOU MAY:

A. use the Software in the manner described in the Software documentation and in accordance with the License Module. If the Software is part of an offering containing multiple Software titles, the aggregate number of copies You may use may not exceed the aggregate number of licenses indicated in the License Module, as calculated by any combination of licensed Software titles in such offering. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software You are authorized to use on a single machine;

B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;

C. use the Software on a network or to protect a network such as at the gateway or on a mail server, provided that You have a license to the Software for each computer that can access the network;

D. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees to the terms of this license; and

E. use the Software in accordance with any additional permitted uses set forth in Section 8 below.

YOU MAY NOT:

A. copy the printed documentation which accompanies the Software;

B. sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. use a previous version or copy of the Software after You have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

D. use a later version of the Software than is provided herewith unless You have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;

E. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received a permission in a License Module;

F. use the Software in any manner not authorized by this license; nor

G. use the Software in any manner that contradicts any additional restrictions set forth in Section 8 below.

2. CONTENT UPDATES:

Certain Symantec software products utilize content that is updated from time to time (antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; some firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as "Content Updates"). You may obtain Content Updates for any period for which You have purchased upgrade insurance for the product, entered into a maintenance agreement that includes Content Updates, or otherwise separately acquired the right to obtain Content Updates. This license does not otherwise permit You to obtain and use Content Updates.

3. LIMITED WARRANTY:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. DISCLAIMER OF DAMAGES:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT

OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether You accept the Software.

5. U.S. GOVERNMENT RESTRICTED RIGHTS:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. EXPORT REGULATION:

Export or re-export of this Software is governed by the laws and regulations of the United States and import laws and regulations of certain other countries Export or re-export of Software to any entity on the Denied Parties List and other lists promulgated by various agencies of the United States Federal Government is strictly prohibited.

7. GENERAL:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. The original of this Agreement has been written in English and English is the governing language of this Agreement. This Agreement may only be modified by a License Module which accompanies this license or by a written document which has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A. or (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland.

8. ADDITIONAL RESTRICTIONS FOR SPECIFIED SOFTWARE:

A. If the Software You have licensed is a specified Symantec AntiVirus™ for a third-party product or platform, You may only use that specified Software with the corresponding product or platform. You may not allow any computer to access the Software other than a computer using the specified product or platform. In the event that You wish to use the Software with a certain product or platform for which there is no specified Software, You may use the Symantec AntiVirus Scan Engine.

B. If the Software you have licensed is Symantec AntiVirus for NetApp® Filer, the following additional use(s) and restriction(s) apply:

i) You may use the Software only with a NetApp Filer server;

ii) You may use the Software only with files accessed through a NetApp Filer; and

iii) You may not use the Software on a server that exceeds the specified capacity set forth in Your License Module.

C. If the Software you have licensed is Symantec AntiVirus for Web Servers, the following additional use(s) and restriction(s) apply:

i) You may use the Software only with files that are received from third parties through a Web server;

ii) You may use the Software only with files received from less than 10,000 unique third parties per month; and

iii) You may not charge or assess a fee for use of the Software for Your internal business.

D. If the Software You have licensed is Symantec Web Security, independent of version or operating platform designation, upon the expiration of Your right to acquire Content Updates, the filtering definitions corresponding with all previous Content Updates will be entirely deleted and will no longer be available for use with the Software. Upon the expiration of Your right to acquire Content Updates, access to updated virus definitions will no longer be available. However, You may continue to use virus definitions previously acquired.

E. If the Software You have licensed is Symantec AntiVirus Corporate Edition, You may not use the Software on or with devices on Your network running embedded operating systems specifically supporting network-attached storage functionality without separately licensing a version of such Software specifically licensed for a specific type of network-attached storage device under a License Module.

F. If the Software You have licensed is Symantec AntiVirus for EMC® Celerra™ File Server, You may use the Software only with EMC Celerra servers and only if You have a license to the Software for each Celerra AntiVirus Agent (CAVA) associated with each such server. You may not allow any computer to access the Software other than an EMC Celerra server.

NetApp is a registered trademark of Network Appliance, Inc., in the U.S. and other countries.

EMC and Celerra are trademarks or registered trademarks of EMC Corporation in the U.S. and other countries.

Contents

Technical support

Chapter 1 Introducing the Symantec AntiVirus Scan Engine

About the Symantec AntiVirus Scan Engine 14
The Symantec AntiVirus Scan Engine solution 14
What's new in version 4.0 16
Where to start 17
Considerations for implementation 18
About Symantec AntiVirus Scan Engine deployment 18
How the scan engine works with the client application 19
About automatic load balancing 20
About supported protocols 20
The native protocol 21
Internet Content Adaptation Protocol (ICAP) 21
Remote procedure call (RPC) 22
About virus protection 22
How viruses are detected 23
Testing virus detection capabilities 25

Chapter 2 Installing the Symantec AntiVirus Scan Engine

System requirements 28
Windows 2000 Server/Advanced Server 28
Solaris 28
Red Hat Linux 28
Preparing for installation 29
Upgrading from previous versions 29
Running other antivirus products on the Symantec AntiVirus Scan Engine server 29
Installing the Symantec AntiVirus Scan Engine 30
Installing on Windows 2000 Server/Advanced Server 31
Installing on Solaris 32
Installing on Red Hat Linux 35
Stopping and restarting the Symantec AntiVirus Scan Engine service 37
Uninstalling the Symantec AntiVirus Scan Engine 38

Chapter 3 Symantec AntiVirus Scan Engine administration

About the administrative interface 42
Built-in HTTP server 42
Virtual administrator account password 43
Accessing the administrative interface 43
About the main administration page 44
Changing the administration settings 47

Chapter 4 Activating product licenses

About licensing 52
License warning and grace periods 52
Removing license files 53
Activating a license 53
Checking the license status 55

Chapter 5 Configuring the Symantec AntiVirus Scan Engine

About configuring the Symantec AntiVirus Scan Engine 58
Selecting the communication protocol 58
Configuring the Symantec AntiVirus Scan Engine native protocol 59
Configuring ICAP 61
Configuring RPC 64
Editing the service startup properties 69
Quarantining unrepairable infected files 70
Allocating resources 72
Activating alerts 77
Activating SNMP alerting 77
Activating SMTP alerting 80

Chapter 6 Setting scanning and blocking policies

About scanning and blocking policies 86
Specifying processing limits 87
Specifying limits for container files 87
Specifying processing limits that apply to all files 90
Configuring antivirus settings 92
Changing the Bloodhound sensitivity level 92
Specifying file types to scan 93
Establishing a mail filter policy 97
Mail filter policy settings 98

Chapter 7 Configuring and using logging

About Symantec AntiVirus Scan Engine logging 110
Configuring standard logging 111
Changing the log file location 111
Specifying what to log 112
Changing the message string file location 116
Managing the standard logs 117
Obtaining summary data from the standard logs 120
Interpreting summary data from the standard logs 121
Generating scanning statistics from the billing logs 121
Interpreting scanning statistics 123
Understanding the 95th percentile bandwidth measurement 124

Chapter 8 Configuring LiveUpdate

About LiveUpdate 126
Updating virus definitions 126
Scheduling LiveUpdate via the command line 128
Setting up your own LiveUpdate server 129

Chapter 9 Customizing log entries and alert messages

About the message string file 132
Editing the message string file 132
About alert strings 133
About alert text for MIME-encoded messages 138
About log entries 141
Editing the ICAP access denied message 143

Chapter 10 Integrating the Symantec AntiVirus Scan Engine with SESA

About SESA 146
Configuring logging to SESA 147
Configuring SESA to recognize the Symantec AntiVirus Scan Engine 147
Installing the local SESA Agent 149
Configuring the scan engine to log events to SESA 153
Scan engine events that are forwarded to SESA 154
Interpreting scan engine events in SESA 155
Uninstalling the SESA integration components 156
Uninstalling the local SESA Agent 156

Appendix A Editing the configuration file

Editing the Symantec AntiVirus Scan Engine configuration file 158
Configuration options 159
Changing protocol-specific settings via the configuration file 159
Changing resource allocation via the configuration file 163
Configuring logging options via the configuration file 165
Configuring alerting via the configuration file 167
Changing the administration settings via the configuration file 169
Specifying processing limits via the configuration file 171
Changing the antivirus settings via the configuration file 172
Blocking MIME partial message content 174
Activating mail message body updates 174
Scheduling LiveUpdate to occur automatically 175
Extracting all streams from OLE structured storage documents for scanning 175

Appendix B Reviewing scanning statistics from the command line

Using the getstat utility 178
Interpreting getstat utility data 179

Appendix C Return codes

Native protocol return codes 182
ICAP version 0.95 return codes 183
ICAP version 1.0 return codes 183
RPC return codes 184

Appendix D Using the silent install feature

About the silent install feature 186
Creating the response file 186
Creating the response file on Windows 2000 Server/Advanced Server 186
Creating the response file on Solaris and Linux 187
Initiating the silent install using the response file 190
Using the silent install feature for uninstall 191

Index

CD Replacement Form

Chapter 1

Introducing the Symantec AntiVirus Scan Engine

This chapter includes the following topics:

- About the Symantec AntiVirus Scan Engine
- Where to start
- Considerations for implementation
- About supported protocols
- About virus protection

About the Symantec AntiVirus Scan Engine

The Symantec AntiVirus Scan Engine, formerly marketed as CarrierScan Server, is a carrier-class virus scanning and repair engine. The Symantec AntiVirus Scan Engine features all of the key virus-scanning technologies available in the complete line of Symantec antivirus products, making the Symantec AntiVirus Scan Engine one of the most effective virus solutions available for detecting and preventing virus attacks.

The Symantec AntiVirus Scan Engine provides virus scanning and repair capabilities to any application on an IP network, regardless of platform, using one of three protocols. Any application can pass files to the Symantec AntiVirus Scan Engine for scanning, which in turn scans the files for viruses and returns a cleaned file if necessary.

The Symantec AntiVirus Scan Engine accepts scan requests from client applications using one of three protocols. The scan engine has its own native protocol, and also can accept scan requests via a proprietary implementation of the remote procedure call (RPC) protocol and the Internet Content Adaptation Protocol (ICAP). The Symantec AntiVirus Scan Engine native protocol includes a client-side application program interface (API) C library for easy integration. The Symantec AntiVirus Scan Engine software development kit (SDK) is available for custom integration using version 2.0 of the native protocol or the December 2001 draft standard version 1.0 of ICAP. Symantec also has developed connector code for some third-party applications for seamless integration with the Symantec AntiVirus Scan Engine.

The Symantec AntiVirus Scan Engine solution

The Symantec AntiVirus Scan Engine satisfies the following key needs of Internet infrastructure organizations:

- Scalability: The Symantec AntiVirus Scan Engine can run on existing computers in your organization's infrastructure or on one or more separate computers on the network. Additional computers that run the scan engine can easily be added at any time to handle increased loads. The Symantec AntiVirus Scan Engine API provides automatic load balancing for multiple scan engines that are running on the network.
- Robustness: If the scan engine goes down for any reason, it automatically restarts, making the Symantec AntiVirus Scan Engine ideal for Internet environments that are always on.
- Speed: The Symantec AntiVirus Scan Engine uses the Symantec AntiVirus™ engine, which is one of the fastest in the industry.

- Virus protection: In addition to the virus protection capabilities available in all Symantec antivirus products, the Symantec AntiVirus Scan Engine offers controls to help prevent denial of service attacks that are caused by container files that are overly large or that contain multiple embedded compressed files.
- Serviceability: Virus definitions for the Symantec AntiVirus Scan Engine can be automatically updated without interruption in virus scanning, on all platforms. The Symantec AntiVirus Scan Engine supports Symantec LiveUpdate™ technology.
- Manageability: The Symantec AntiVirus Scan Engine can be remotely managed from any computer on your network via a Web-based administrative interface. The Symantec AntiVirus Scan Engine provides full-featured logging and SMTP (simple mail transfer protocol) and SNMP (simple network management protocol) alerting capability for a full range of activity, making it manageable in large environments.
- Multiple protocol support: The Symantec AntiVirus Scan Engine accepts scan requests from client applications using one of three protocols:
  - The Symantec AntiVirus Scan Engine native protocol
  - The Internet Content Adaptation Protocol (ICAP), version 0.95 (proprietary implementation) and the December 2001 draft standard version 1.0
  - A proprietary implementation of remote procedure call (RPC)
- Ease of integration: The Symantec AntiVirus Scan Engine runs on Sun® Solaris®, Red Hat® Linux®, and Microsoft® Windows® 2000 Server and 2000 Advanced Server platforms. Because the scan engine can run on a separate computer on the network, it can easily be deployed in any environment that is running any set of platforms. If you want to use the native protocol to do your own integration, a client-side API can be used to add virus scanning to any C or C++ application. If you want to use version 1.0 of ICAP, the protocol specification is available. To make integration with some third-party applications convenient and easy, Symantec also provides a number of connectors for the Symantec AntiVirus Scan Engine.
- Billing support: The Symantec AntiVirus Scan Engine maintains bandwidth utilization statistics and file-scanning statistics to facilitate different billing schemes.

What's new in version 4.0

The Symantec AntiVirus Scan Engine version 4.0 includes the following new features:

- Support for antivirus scanning via ICAP version 1.0: The Symantec AntiVirus Scan Engine now provides simultaneous support for both version 0.95 and the December 2001 draft version 1.0 of ICAP.
- Support for multiple RPC clients via the RPC protocol: A single Symantec AntiVirus Scan Engine can now provide simultaneous antivirus scanning support for multiple RPC clients.
- Logging of events and alerts to the Symantec Enterprise Security Architecture (SESA): SESA permits centralized viewing and management of security information generated on computers that are running Symantec security products. If you have purchased SESA, the Symantec AntiVirus Scan Engine can be configured to log events and alerts to SESA.
- Integration of the Symantec Enterprise Licensing System (ELS): Key features of the Symantec AntiVirus Scan Engine are now activated by license key, including antivirus scanning functionality and virus definitions downloads.
- Quarantining of infected files that cannot be repaired: Infected files that cannot be repaired can be forwarded to a separately installed Symantec Central Quarantine and isolated so that the viruses cannot spread. From the Quarantine, the files can be submitted to Symantec Security Response for analysis. This feature is currently available only when the RPC protocol is in use.

Where to start

The *Symantec AntiVirus Scan Engine Implementation Guide* contains all of the instructions necessary to install and maintain the Symantec AntiVirus Scan Engine. Follow these steps to ensure that you use the scan engine's capabilities effectively:

- Become familiar with the design and features of the software.
  See "Introducing the Symantec AntiVirus Scan Engine" on page 13.
- Decide how to deploy the Symantec AntiVirus Scan Engine on your network to meet your specific requirements. If you plan to use the native protocol or ICAP version 1.0 to create a custom implementation of the scan engine and have purchased the Symantec AntiVirus Scan Engine SDK, the *Symantec AntiVirus Scan Engine Software Developer's Guide* contains additional information on deploying the scan engine using these protocols. If you have purchased a specific connector for the Symantec AntiVirus Scan Engine, check the accompanying documentation for additional information on that particular implementation of the scan engine.
  See "Considerations for implementation" on page 18.
- Install the Symantec AntiVirus Scan Engine. Verify that your system meets the minimum requirements before installing.
  See "Installing the Symantec AntiVirus Scan Engine" on page 27.
- Activate the licenses for key features for the Symantec AntiVirus Scan Engine, including antivirus scanning functionality and virus definitions updates, through the Symantec AntiVirus Scan Engine administrative interface.
  See "Activating product licenses" on page 51.
- Review the configuration information in Chapters 5–10 of this guide to fully customize the Symantec AntiVirus Scan Engine to meet your needs. This includes configuring LiveUpdate™, so that the scan engine always has the necessary information to detect and remove newly discovered viruses.
- Configure the client applications that will send files for scanning to the Symantec AntiVirus Scan Engine. If you purchased the Symantec AntiVirus Scan Engine SDK, the *Symantec AntiVirus Scan Engine Software Developer's Guide* provides this information. If you have purchased a specific connector for the Symantec AntiVirus Scan Engine, see the documentation for that connector for instructions on configuring the client application.

Considerations for implementation

The Symantec AntiVirus Scan Engine can be easily implemented into an existing infrastructure. The Symantec AntiVirus Scan Engine runs on Solaris, Red Hat Linux, and Windows 2000 Server platforms.

See "About Symantec AntiVirus Scan Engine deployment" on page 18.

Symantec provides connectors for some third-party products for seamless integration with the Symantec AntiVirus Scan Engine.

See "How the scan engine works with the client application" on page 19.

For custom integration using the native protocol, the Symantec AntiVirus Scan Engine features a client-side API, which streamlines the integration of antivirus scanning for any C or C++ application. The Symantec AntiVirus Scan Engine API provides scheduling across any number of computers that are running the Symantec AntiVirus Scan Engine.

See "About automatic load balancing" on page 20.

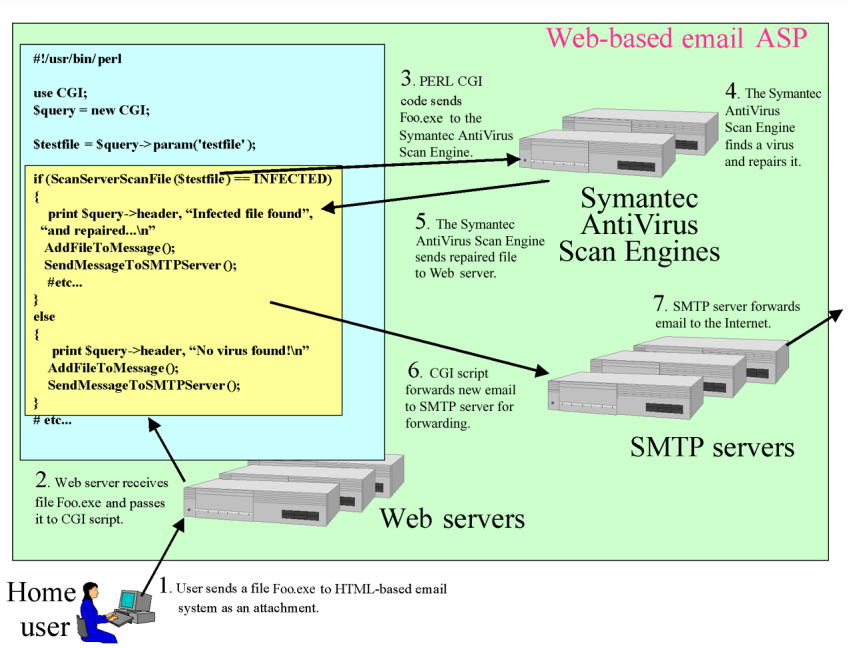
About Symantec AntiVirus Scan Engine deployment

In a typical configuration, files are passed to the Symantec AntiVirus Scan Engine via a socket over the network because the scan engine is running on a separate computer. Depending on the network setup, client applications (applications that have been configured to pass files to the scan engine for scanning) can pass a full path rather than the actual file to the Symantec AntiVirus Scan Engine. For example, files to be scanned may be located on a drive that can be mounted over the network, such as a shared drive in Windows or a network file system (NFS) drive. If the client application and the scan engine have access to a shared directory, the client application can place the file in the shared directory and pass the full path to the Symantec AntiVirus Scan Engine, which can access the file directly.

For cases in which the client application is running on the same computer as the Symantec AntiVirus Scan Engine, the client application can pass the file name to the scan engine, and the scan engine can open the file and scan it in place on the computer.

One example of a typical integration of the Symantec AntiVirus Scan Engine is shown in Figure 1-1. Integration scenarios are discussed in detail in *Symantec CarrierScan Server Version 2.0: A Symantec White Paper,* which is available on the Symantec Web site.

Figure 1-1 Typical integration of the Symantec AntiVirus Scan Engine


Web-based email ASP
#!/usr/bin/perl
use CGI;
$query = new CGI;
$testfile = $query->param('testfile');
if (ScanServerScanFile ($testfile) == INFECTED)
{
print $query->header, "Infected file found",
"and repaired...\n"
AddFileToMessage();
SendMessageToSMTPServer();
#etc...
}
else
{
print $query->header, "No virus found!\n"
AddFileToMessage();
SendMessageToSMTPServer();
}
# etc...
3. PERL CGI code sends Foo.exe to the Symantec AntiVirus Scan Engine.
4. The Symantec AntiVirus Scan Engine finds a virus and repairs it.
Symantec AntiVirus Scan Engines
5. The Symantec AntiVirus Scan Engine sends repaired file to Web server.
7. SMTP server forwards email to the Internet.
6. CGI script forwards new email to SMTP server for forwarding.
SMTP servers
2. Web server receives file Foo.exe and passes it to CGI script.
Web servers
Home user
1. User sends a file Foo.exe to HTML-based email system as an attachment.

How the scan engine works with the client application

The Symantec AntiVirus Scan Engine is designed to be easily integrated into any environment to provide antivirus scanning for any application. Client applications are configured to pass files, via one of three protocols, to the Symantec AntiVirus Scan Engine, which scans the files for viruses and returns cleaned files if necessary.

Depending on the protocol that is used, the Symantec AntiVirus Scan Engine can be configured to scan only certain file types that are passed to it by client applications. In other cases, the client application must decide what to scan and what to do with the results.

If you want to use the native protocol to do your own integration, a client-side API can be used to add virus scanning to any C or C++ application. If you want to use ICAP version 1.0 to do your own integration, the specification is available. To make integration with some third-party applications convenient and easy, Symantec also provides a number of connectors for the Symantec AntiVirus Scan Engine. Other software companies may develop connectors for the Symantec AntiVirus Scan Engine to provide antivirus scanning for their own products.

If you have purchased the Symantec AntiVirus Scan Engine with a connector, you may need to configure the Symantec AntiVirus Scan Engine to work with the connector. You may need to configure the application to add virus scanning as well. You will need the information that is contained in the *Symantec AntiVirus Scan Engine Implementation Guide* and any additional documentation that is included with the connector.

About automatic load balancing

The Symantec AntiVirus Scan Engine API provides scheduling across any number of computers that are running the Symantec AntiVirus Scan Engine. Client applications that pass files to the scan engine benefit from load-balanced virus scanning without any additional effort. The API determines the appropriate Symantec AntiVirus Scan Engine (when multiple scan engines are used) to receive the next file to be scanned, based on the scheduling algorithm.

If a Symantec AntiVirus Scan Engine is unreachable or goes down during a scan, another scan engine is called and the faulty scan engine is taken out of rotation for a period of time. If all of the scan engines are out of rotation, the faulty scan engines are called again. The API does not stop trying to contact the scan engine unless five engines are not functioning or it appears that a file that is being scanned might have caused more than one engine to go down.

Note: If you are using the Symantec AntiVirus Scan Engine as a plug-in using RPC or ICAP, load balancing across multiple scan engines may be configurable, depending on the implementation. See the plug-in documentation.

About supported protocols

The Symantec AntiVirus Scan Engine lets client applications send scan requests using one of three protocols:

- The native protocol
- The Internet Content Adaptation Protocol (ICAP)
- A proprietary remote procedure call (RPC) protocol

The protocol can be changed at any time.

See "Selecting the communication protocol" on page 58.

The native protocol

In the default configuration, the Symantec AntiVirus Scan Engine implements a simple TCP/IP protocol to provide antivirus functionality to client applications. This protocol is text-based, like HTTP or SMTP, and uses standard ASCII commands and responses to communicate between client and server.

To scan a file, a client connects to IP port 7777 (the default), sends the file to be scanned, and then reads the results of the scan. After receiving the scan results, the client and server disconnect and must initiate new connections to scan subsequent files.

See "Configuring the Symantec AntiVirus Scan Engine native protocol" on page 59.

Internet Content Adaptation Protocol (ICAP)

ICAP is a lightweight protocol for executing a remote procedure call on HTTP messages. ICAP is part of an evolving architecture that lets corporations, carriers, and ISPs dynamically scan, change, and augment Web content as it flows through ICAP servers. The protocol lets ICAP clients pass HTTP messages to ICAP servers for adaptation (some sort of transformation or other processing, such as virus scanning). The server executes its transformation service on messages and responds to the client, usually with modified messages. The adapted messages may be either HTTP requests or HTTP responses.

In a typical integration, a caching proxy server retrieves requested information from the Web. At the same time, it caches the information (stores a copy on disk), and, where possible, serves multiple requests for the same Web content from the cache. A caching proxy server can use ICAP to communicate with the Symantec AntiVirus Scan Engine and request scan and repair of content that is retrieved from the Web. The Symantec AntiVirus Scan Engine uses the proprietary version 0.95 implementation and the December 2001 draft standard version 1.0 of ICAP, depending on the requesting client.

See "Configuring ICAP" on page 61.

Remote procedure call (RPC)

Remote procedure call (RPC) is a client/server infrastructure that increases the interoperability and portability of an application by letting the application be distributed over multiple platforms. The use of RPC frees the developer from having to be familiar with various operating system and network interfaces, and simplifies the development of applications that span multiple operating systems and network protocols. Complexity is significantly reduced by keeping the semantics of a remote call the same whether or not the client and server are located on the same computer.

The Symantec AntiVirus Scan Engine can be configured to use a proprietary virus scanning protocol with the MS-RPC protocol (for Windows 2000 Server platforms only) to interface with client applications. Any appropriate client can use RPC to communicate with the Symantec AntiVirus Scan Engine and request scanning and repairing of files.

See "Configuring RPC" on page 64.

About virus protection

The Symantec AntiVirus Scan Engine features all of the virus scanning technologies that are available in Symantec antivirus products. The Symantec AntiVirus Scan Engine detects viruses, worms, and Trojan horses in all major file types (for example, Windows files, DOS files, and Microsoft Word and Excel files). The Symantec AntiVirus Scan Engine also includes a decomposer that handles most compressed and archive file formats and nested levels of files. You can configure the scan engine to limit scanning to certain file types based on file extension.

To protect against container files that can cause denial of service attacks (for example, container files that are overly large, that contain large numbers of embedded compressed files, or that have been designed to use resources maliciously and degrade performance), the Symantec AntiVirus Scan Engine lets you specify the maximum amount of time that the scan engine devotes to decomposing a container file and its contents, the maximum file size for individual files in a container file, and the maximum number of nested levels to be decomposed for scanning.

The Symantec AntiVirus Scan Engine also detects mobile code such as Java™, ActiveX®, and standalone script-based threats. The Symantec AntiVirus Scan Engine utilizes Symantec antivirus technologies, including Bloodhound™, for heuristic detection of new or unknown viruses; NAVEX™, which provides protection from new classes of viruses automatically via LiveUpdate; and Striker, for the detection of polymorphic viruses.

If you would like to know whether the Symantec AntiVirus Scan Engine or any other Symantec product protects against a specific virus, visit the Symantec Security Response™ Web site at:

http://securityresponse.symantec.com

The Symantec AntiVirus Scan Engine technology is supported by the Symantec Security Response team. These Symantec engineers work 24 hours per day, 7 days per week, tracking new virus outbreaks and identifying new virus threats.

How viruses are detected

When Symantec engineers identify a new virus, information about the virus (a virus signature) is stored in a virus definitions file. Virus definitions files are updated periodically via the Symantec automated LiveUpdate feature. When the Symantec AntiVirus Scan Engine scans for viruses, it searches for these virus signatures. To supplement the detection of virus infections by virus signature, the Symantec AntiVirus Scan Engine includes Bloodhound technology, which heuristically detects new or unknown viruses based on the general characteristics exhibited by known viruses.

About Bloodhound heuristic technology

Symantec engineers have developed two types of heuristics for the detection of unknown viruses. The first, Bloodhound, is capable of detecting upwards of 80 percent of new and unknown executable file viruses. The second, Bloodhound-Macro, detects and repairs over 90 percent of new and unknown macro viruses. Bloodhound requires minimal overhead since it examines only programs and documents that meet stringent prerequisites. In most cases, Bloodhound can determine in microseconds whether a file or document is likely to be infected by a virus. If it determines that a file is not able to be infected, it immediately moves to the next file.

Bloodhound and executable viruses

Bloodhound uses artificial intelligence (AI) technology to isolate and locate the various logical regions of each application that it is told to scan. It analyzes the program logic in each of these regions for virus-like behavior and simulates this behavior to determine whether the program is a virus.

Bloodhound and macro viruses

Symantec Bloodhound-Macro technology uses a hybrid heuristic scheme to detect and repair more than 90 percent of all new and unknown macro viruses automatically. For example, every time that the Symantec AntiVirus Scan Engine scans a Microsoft Word document, Bloodhound-Macro sets up a complete

virtual Word environment into which it loads the document. The macros that are contained in the document are run as they would be in the word processing application.

Bloodhound-Macro monitors the macros as they run to see if they copy themselves from the host document to another virtual document. Bloodhound-Macro also runs the copied macros and verifies that they can further propagate.

About NAVEX technology

NAVEX is a technology that lets the Symantec Security Response team update the antivirus scanning component of the Symantec AntiVirus Scan Engine during routine virus definitions updates. This means that no inline revisions or time-consuming upgrades are necessary to ensure that your antivirus protection stays current, regardless of platform, even against new virus threats.

The antivirus scanning component is made up of dozens of complex search algorithms, CPU emulators, and other program logic. The scanning component examines a file to determine whether it contains viruses. The scanning component scans files and disks for virus fingerprints (unique sequences of bytes that are known to be contained in viruses). These fingerprints are stored in the virus definitions files that are downloaded at least once per week. The scanning component also repairs infected files.

Occasionally, a new virus or class of viruses emerges that cannot be detected by existing scanning components. These viruses require new algorithms for detection, and consequently a new scanning component. With the NAVEX technology, Symantec engineers can quickly upgrade the Symantec AntiVirus scanning components, with no extra cost or effort required.

Striker technology

Striker technology identifies polymorphic computer viruses, which are the most complex and difficult viruses to detect. Like an encrypted virus, a polymorphic virus includes a scrambled virus body and a decryption routine that first gains control of the computer, and then decrypts the virus body. However, a polymorphic virus also adds a mutation engine that generates randomized decryption routines that change each time that a virus infects a new program. As a result, no two polymorphic viruses are the same.

Each time that Striker scans a new program file, it loads the file into a self-contained virtual computer. The program executes in this virtual computer as if it were running on a real computer. The polymorphic virus runs and decrypts itself. Striker then scans, detects, and repairs the virus.

LiveUpdate

LiveUpdate ensures that your network is not at risk of infection by newly discovered viruses. Updated virus definitions files, which contain the necessary information to detect and eliminate viruses, are supplied by Symantec at least every week and whenever a new virus threat is discovered. The Symantec AntiVirus Scan Engine can be configured to poll the Symantec LiveUpdate servers to determine whether updated virus definitions have been posted. If new virus definitions are available, the Symantec AntiVirus Scan Engine downloads the files and installs them in the proper location. Virus protection stays current without any interruption in protection.

Testing virus detection capabilities

If you want to verify the virus detection capabilities of the Symantec AntiVirus Scan Engine, visit the following Web site:

http://www.eicar.org

The site provides a link to a test virus that should be detected by all major antivirus vendors.

Warning: Carefully read the disclaimers on the site prior to downloading the test file into your environment. Any attempts to test antivirus software with real or dummy viruses should be handled with extreme care.

If your computer already has antivirus software, you must disable the auto-protect mode of the antivirus software before downloading the test file.

Chapter 2

Installing the Symantec AntiVirus Scan Engine

This chapter includes the following topics:

- System requirements
- Preparing for installation
- Installing the Symantec AntiVirus Scan Engine
- Stopping and restarting the Symantec AntiVirus Scan Engine service
- Uninstalling the Symantec AntiVirus Scan Engine

System requirements

Before you attempt to install the Symantec AntiVirus Scan Engine, verify that your server meets the system requirements.

Windows 2000 Server/Advanced Server

- Windows 2000 Server with Service Pack 2 or Windows 2000 Advanced Server with Service Pack 2
- Pentium III 500 MHz or higher
- 256+ MB of RAM
- 25 MB of hard disk space
- 1 NIC running TCP/IP with a static IP address
- Microsoft Internet Explorer 6.0 or later for Web-based administration
- Internet connection for LiveUpdate of virus definitions

Solaris

- Solaris 7 or later
- Sun Ultra 10 or higher
- SPARC® 400 MHz or higher
- 256+ MB of RAM
- 35 MB of hard disk space
- 1 NIC running TCP/IP with a static IP address
- Microsoft Internet Explorer 6.0 or later for Web-based administration
- Internet connection for LiveUpdate of virus definitions

Red Hat Linux

- Red Hat Linux version 7.2 or 7.3
- Pentium III 500 MHz or higher
- 256+ MB of RAM
- 25 MB of hard disk space
- 1 NIC running TCP/IP with a static IP address

- Microsoft Internet Explorer 6.0 or later for Web-based administration
- Internet connection for LiveUpdate of virus definitions

Preparing for installation

Before installing the Symantec AntiVirus Scan Engine, you may need to do the following:

- Uninstall the previous version if you are upgrading.
- Consider running an antivirus product to protect the server that is running the Symantec AntiVirus Scan Engine.

Upgrading from previous versions

If you are upgrading the Symantec AntiVirus Scan Engine, you must uninstall the previous version first. To uninstall a previous version, see the documentation for that product.

Note: The Symantec AntiVirus Scan Engine is also an upgrade to Symantec CarrierScan Server. To upgrade, you must uninstall Symantec CarrierScan Server. See the Symantec CarrierScan Server documentation.

Running other antivirus products on the Symantec AntiVirus Scan Engine server

By design, the Symantec AntiVirus Scan Engine scans only files from client applications that are configured to pass files to the scan engine. The Symantec AntiVirus Scan Engine does not protect the computer on which it is running. Because the server on which the Symantec AntiVirus Scan Engine is running handles viruses, the server is vulnerable (if the server has no real-time virus protection of the operating system).

To achieve comprehensive virus protection with the Symantec AntiVirus Scan Engine, it is important to protect the Symantec AntiVirus Scan Engine server from virus attacks. To protect the host computer, run Symantec AntiVirus Corporate Edition on the server that is running the Symantec AntiVirus Scan Engine.

Warning: To prevent a conflict between the Symantec AntiVirus Scan Engine and the antivirus product that is running on the host computer, you must configure the antivirus product on the host computer so that it does not scan the temporary directory that is used by the Symantec AntiVirus Scan Engine for scanning.

Installing the Symantec AntiVirus Scan Engine

The Symantec AntiVirus Scan Engine should be installed on a computer that meets the system requirements.

See "System requirements" on page 28.

Ensure that your server's operating system software and applicable updates are installed, configured, and working correctly before you install the Symantec AntiVirus Scan Engine. Consult your server's documentation for more information.

In most cases, a single instance of the Symantec AntiVirus Scan Engine is installed on a computer. Solaris and Linux permit multiple instances of the Symantec AntiVirus Scan Engine on a single computer, provided that each service has a unique port number and a unique virus definition product name (so that each scan engine can obtain updated virus definitions files). When you are planning to run multiple copies of the scan engine on a single computer, projected scan volume and performance impact should be taken into account.

Once you have installed the Symantec AntiVirus Scan Engine, you must activate all applicable product licenses. You must also activate your subscription to virus definitions updates. The antivirus scanning features are not active until you activate the licenses.

See "Activating product licenses" on page 51.

If you are installing multiple Symantec AntiVirus Scan Engines, you may want to take advantage of the silent install feature for the scan engine.

See "Using the silent install feature" on page 185.

Installing on Windows 2000 Server/Advanced Server

Only a single instance of the Symantec AntiVirus Scan Engine can be run on Windows 2000 Server computers.

To install the Symantec AntiVirus Scan Engine on Windows 2000 Server/ Advanced Server

1. Log on to the computer on which you plan to install Symantec AntiVirus Scan Engine as administrator or with administrator rights.
2. Copy the ScanEngine.exe file from the CD onto the computer.
3. Run the .exe file.
4. Indicate that you agree with the terms of the Symantec license agreement, then click **Next**.

   If you indicate No, the installation is aborted.
5. Select the location in which to install the Symantec AntiVirus Scan Engine, then click **Next**.

   The default location is C:\Program Files\Symantec\Scan Engine.
6. Select one of the following communication protocols:
   - NATIVE
   - ICAP
   - RPC

     If you select RPC as the communication protocol, type the IP address for the RPC client, and then type the account name and password to identify the account (with Backup Operator privileges on the RPC client) on which the Symantec AntiVirus Scan Engine will run.

     If the Symantec AntiVirus Scan Engine is to support multiple RPC clients, you can add additional clients through the scan engine administrative interface. Only one RPC client can be specified at installation.

     The default account is LocalSystem. If you accept the default account, you do not need to enter the password. Use the following format for the account name: domain\username. Make sure that the account has the appropriate permissions. You will not receive an error message if the account does not have appropriate permissions.

     See "Editing the service startup properties" on page 69.
7. Click **Next**.

8 Select the port number on which the Web-based administrative interface listens.

The default port number is 8004. Type **0** to disable the administrative interface.

Note: If you disable the administrative interface, you must configure the Symantec AntiVirus Scan Engine by editing the configuration file.

See "Editing the configuration file" on page 157.

---

9 Type a password for the virtual administrative account that you will use to manage the Symantec AntiVirus Scan Engine.

10 Confirm the password by typing it again.

11 Click **Next**.

12 To log scan engine events to the Symantec Enterprise Security Architecture (SESA), do all of the following:

- Check **Enable SESA support**.
- In the SESA Manager IP address or host name box, type the IP address or host name of the computer on which the SESA Manager is running.
- In the SESA Manager port box, type the port number on which the SESA Manager listens.

  The default port number is 443.

See "Integrating the Symantec AntiVirus Scan Engine with SESA" on page 145.

The installer proceeds from this point with the installation. When the installation is complete, the Symantec AntiVirus Scan Engine is installed as a Windows 2000 service, and is listed as Symantec AntiVirus Scan Engine in the Services Control Panel. Significant installation activities are recorded in the Application Event Log.

Installing on Solaris

The Solaris version of the Symantec AntiVirus Scan Engine is distributed as a self-extracting, self-installing shell archive (shar) named ScanEngine.sh.

To install the Symantec AntiVirus Scan Engine on Solaris

1 Log on as root to the computer on which you plan to install the Symantec AntiVirus Scan Engine.

2 Copy the distribution file, ScanEngine.sh, from the CD onto the computer.

3 Change directories to the location in which you copied the distribution file.

4 Type the following command, then press **Enter**:
sh ./ScanEngine.sh

5 Indicate that you agree with the terms of the Symantec license agreement, then press **Enter**.
If you indicate No, the installation is aborted.

6 Indicate whether to create the avdefs group.
The avdefs group has access rights to the directory that contains the virus definitions that are used by the Symantec AntiVirus Scan Engine. If you have previously installed a Symantec product on the computer, this group may already exist. If so, this option is not available.

7 Select the location in which to install the Symantec AntiVirus Scan Engine, then press **Enter**.
The default location is /opt/SYMCScan.

8 Indicate whether to create the SymShared directory.
The SymShared directory contains the virus definitions that are used by the Symantec AntiVirus Scan Engine to scan for viruses. The default location is /opt/Symantec. If you have multiple Symantec products installed on the computer, this directory lets the products share virus definitions. If you have previously installed a Symantec product on the computer, this directory may already exist. If so, this option is not available.

9 Select the protocol to be used by the Symantec AntiVirus Scan Engine, then click **Next**.

10 Select the port number on which the Web-based administrative interface listens.
The default port number is 8004. Type **0** to disable the administrative interface.

Note: If you disable the administrative interface, you must configure the Symantec AntiVirus Scan Engine by editing the configuration file.
See "Editing the configuration file" on page 157.

---

11 Type a password for the virtual administrative account that you will use to manage the Symantec AntiVirus Scan Engine.

12 Confirm the password by typing it again.

13 To log scan engine events to the Symantec Enterprise Security Architecture (SESA), do all of the following:

- At the Does this system use the Symantec Enterprise Security Architecture (SESA) prompt, type **y** for yes.
- Type the IP address or host name of the computer on which the SESA Manager is running, then press **Enter**.
- Type the port number on which the SESA Manager listens, then press **Enter**.

  The default port number is 443.

See "Integrating the Symantec AntiVirus Scan Engine with SESA" on page 145.

The installer proceeds from this point with the installation. The Symantec AntiVirus Scan Engine starts automatically as a daemon (service) when the installation is complete. A transcript of the installation is saved as /var/log/SYMCScan-install.log for later review.

To ensure that the Symantec AntiVirus Scan Engine daemon is running on Solaris

1 Type the following command:

ps -ea | grep sym

2 Press **Enter**.

You should see a list of processes similar to the following:

5358 ?0:00 symcscan
5359 ?0:00 symcscan

If nothing is displayed, the Symantec AntiVirus Scan Engine daemon did not start.

3 If the Symantec AntiVirus Scan Engine daemon did not start, type the following command:

/etc/init.d/symcscan restart

Installing on Red Hat Linux

The Red Hat Linux version of the Symantec AntiVirus Scan Engine is distributed as a self-extracting, self-installing shell archive (shar) named ScanEngine.sh.

Note: If you are installing the Symantec AntiVirus Scan Engine on Red Hat Linux version 7.3, you must first install the C++ compatible libraries. These libraries are included in the Red Hat Linux distribution. They are contained in the compat-libstdc++6.2-2.9.0.16 RPM. If these libraries are not installed, the scan engine will not install.

To install the Symantec AntiVirus Scan Engine on Red Hat Linux

1. Log on as root to the computer on which you plan to install the Symantec AntiVirus Scan Engine.
2. Copy the distribution file, ScanEngine.sh, from the CD onto the computer.
3. Change directories to the location in which you copied the distribution file.
4. Type the following command, then press **Enter**:
   sh ./ScanEngine.sh
5. Indicate that you agree with the terms of the Symantec license agreement, then press **Enter**.
   If you indicate No, the installation is aborted.
6. Indicate whether to create the avdefs group.
   The avdefs group has access rights to the directory that contains the virus definitions that are used by the Symantec AntiVirus Scan Engine. If you have previously installed a Symantec product on the computer, this group may already exist. If so, this option is not available.
7. Select the location in which to install the Symantec AntiVirus Scan Engine, then press **Enter**.
   The default location is /opt/SYMCScan.
8. Indicate whether to create the SymShared directory.
   The SymShared directory contains the virus definitions that are used by the Symantec AntiVirus Scan Engine to scan for viruses. The default location is /opt/Symantec. If you have multiple Symantec products installed on the computer, this directory lets the products share virus definitions. If you have previously installed a Symantec product on the computer, this directory may already exist. If so, this option is not available.

9 Select the protocol to be used by the Symantec AntiVirus Scan Engine, then click **Next**.

10 Select the port number on which the Web-based administrative interface listens.

The default port number is 8004. Type **0** to disable the administrative interface.

Note: If you disable the administrative interface, you must configure the Symantec AntiVirus Scan Engine by editing the configuration file.

See "Editing the configuration file" on page 157.

---

11 Type a password for the virtual administrative account that you will use to manage the Symantec AntiVirus Scan Engine.

12 Confirm the password by typing it again.

13 To log scan engine events to the Symantec Enterprise Security Architecture (SESA), do all of the following:

- At the Does this system use the Symantec Enterprise Security Architecture (SESA) prompt, type **y** for yes.
- Type the IP address or host name of the computer on which the SESA Manager is running, then press **Enter**.
- Type the port number on which the SESA Manager listens, then press **Enter**.

  The default port number is 443.

See "Integrating the Symantec AntiVirus Scan Engine with SESA" on page 145.

The installer proceeds from this point with the installation. The Symantec AntiVirus Scan Engine starts automatically as a daemon (service) when installation is complete. A transcript of the installation is saved as /var/log/SYMCScan-install.log for later review.

To ensure that the Symantec AntiVirus Scan Engine daemon is running on Linux

1. Type the following command:
   ps -ea | grep sym
2. Press **Enter**.
   You should see a list of processes similar to the following:
   5358 ?0:00 symcscan
   5359 ?0:00 symcscan
   The list of processes that is displayed may be longer than the list shown here. If nothing is displayed, the Symantec AntiVirus Scan Engine daemon did not start.
3. If the Symantec AntiVirus Scan Engine daemon did not start, type the following command:
   /etc/rc.d/init.d/symcscan restart

Stopping and restarting the Symantec AntiVirus Scan Engine service

You may need to stop and restart the Symantec AntiVirus Scan Engine service. Stopping and restarting the Symantec AntiVirus Scan Engine service results in a lost connection to client applications that are in the process of submitting a file for scanning. The client application must reestablish the connection and resubmit the file for scanning.

To stop and restart the Symantec AntiVirus Scan Engine service

Instructions for stopping and restarting the Symantec AntiVirus Scan Engine service differ depending on the operating system that you are running. If you are running the Symantec AntiVirus Scan Engine on Windows 2000 Server/ Advanced Server, stop and start service in the Services Control Panel.

To stop and restart the Symantec AntiVirus Scan Engine service on Solaris

- At the command prompt, do one of the following:
  - To stop the service, type the following command:
    /etc/init.d/symcscan stop
  - To start the service, type the following command:
    /etc/init.d/symcscan start

- To stop and immediately restart the service, type the following command:
  /etc/init.d/symcscan restart

To stop and restart the Symantec AntiVirus Scan Engine service on Linux

- At the command prompt, do one of the following:
  - To stop the service, type the following command:
    /etc/rc.d/init.d/symcscan stop
  - To start the service, type the following command:
    /etc/rc.d/init.d/symcscan start
  - To stop and immediately restart the service, type the following command:
    /etc/rc.d/init.d/symcscan restart

Uninstalling the Symantec AntiVirus Scan Engine

Use the following instructions for uninstalling the Symantec AntiVirus Scan Engine.

Note: Uninstalling the Symantec AntiVirus Scan Engine does not remove the license keys for the Symantec AntiVirus Scan Engine. If you are uninstalling the Symantec AntiVirus Scan Engine permanently, you must manually uninstall the license keys.

To uninstall the Symantec AntiVirus Scan Engine

Uninstallation instructions differ depending on the operating system that you are running.

To uninstall the Symantec AntiVirus Scan Engine on Windows 2000 Server/ Advanced Server

1. In the Add/Remove Programs Control Panel, click **Symantec AntiVirus Scan Engine**.
2. Click **Change/Remove**.
3. Follow the on-screen prompts to complete the uninstallation.

To uninstall the Symantec AntiVirus Scan Engine on Solaris

1. Log on to the computer as root.
2. At the command prompt, type the following command:
   pkgrm SYMCScan
3. Press **Enter**.
4. Follow the on-screen prompts to complete the uninstallation.

To uninstall the Symantec AntiVirus Scan Engine on Red Hat Linux

1. Log on to the computer as root.
2. At the command prompt, type the following command:
   rpm -e SYMCScan
3. Press **Enter**.
4. Follow the on-screen prompts to complete the uninstallation.

Chapter 3

Symantec AntiVirus Scan Engine administration

This chapter includes the following topics:

- About the administrative interface
- Accessing the administrative interface
- Changing the administration settings

About the administrative interface

The Symantec AntiVirus Scan Engine is managed through a Web-based interface. This interface is provided through a built-in HTTP server. The Symantec AntiVirus Scan Engine administrative interface is accessed via a Web browser on any computer on your network that can access the server that is running the Symantec AntiVirus Scan Engine. Microsoft Internet Explorer 6.0 or later is the supported Web browser.

The administrative interface is accessed using a virtual administrative account that is created at installation. The administrative interface lets you manage the Symantec AntiVirus Scan Engine.

In order for changes that have been made through the administrative interface to take effect, you must restart the Symantec AntiVirus Scan Engine service. When you are making changes to the Symantec AntiVirus Scan Engine configuration, remember that stopping and restarting the Symantec AntiVirus Scan Engine service results in a lost connection to client applications that are in the process of submitting files for scanning. (The client application must reestablish the connection and resubmit the file for scanning.) You may want to schedule configuration changes for times when scanning is at a minimum.

Although it is possible for multiple administrative interface sessions to be active at one time for a single Symantec AntiVirus Scan Engine, this practice is strongly discouraged. Having more than one user logged in at the same time can cause possible race conditions, as well as result in conflicting configuration changes being submitted.

Built-in HTTP server

The built-in HTTP server that provides the administrative interface is independent of any existing HTTP server that may be installed on your server and is not a general purpose Web server. During the installation process, you are prompted for the TCP/IP port number on which this built-in HTTP server listens. The port number that you specify must be exclusive to the Symantec AntiVirus Scan Engine administrative interface and must not already be in use by any other program or service.

Because the built-in HTTP server is not a general purpose Web server, do not use port number 80 (the default port number for general purpose Web servers). Unless you have a compelling reason to do otherwise, use the default setting (8004). If you select a port number other than the default, do not forget which port number you chose.

Note: The built-in HTTP server port number differs from the port number on which the Symantec AntiVirus Scan Engine listens for client applications to pass files for scanning. This port number is exclusive to the Symantec AntiVirus Scan Engine administrative interface.

Virtual administrator account password

A virtual administrative account is created at installation. You are also prompted to provide a password for this account during installation. Do not forget the password for this account because the virtual administrative account is the only account that you can use to manage the Symantec AntiVirus Scan Engine. You can change the password via the administrative interface, but you must have the old password to change it.

Accessing the administrative interface

The administrative interface is accessed using a suitable Web browser. Microsoft Internet Explorer 6.0 is the supported Web browser.

When you log on to the administrative interface, the password for the virtual administrative account is unencrypted. For security reasons, you should access the administrative interface using a switch or via a secure segment of the network.

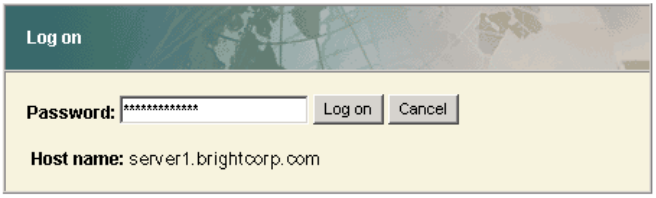
Warning: Although it is possible for multiple administrative interface sessions to be active at one time for a single Symantec AntiVirus Scan Engine, this practice is strongly discouraged. Having more than one user logged in at the same time can cause possible race conditions, as well as result in conflicting configuration changes being submitted.

To access the administrative functions

1. Launch a Web browser on any computer on your network that can access the server that is running the Symantec AntiVirus Scan Engine.
2. Visit the following URL:

   http://<servername>:<port>/

   where <servername> is the host name or IP address of the server that is running the Symantec AntiVirus Scan Engine and <port> is the port number that you selected during installation for the built-in Web server. (8004 is the default port number.)

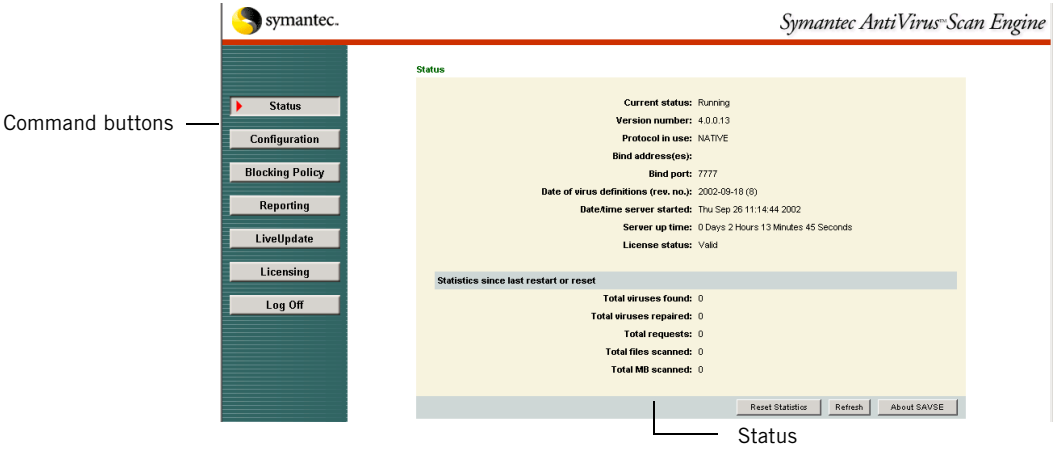


3. In the Log on dialog box, in the Password box, type the password for the administrative account.
4. Click **Log on**.

   The Symantec AntiVirus Scan Engine main administration page displays.

About the main administration page

The main administration page displays command buttons in the left pane and the Symantec AntiVirus Scan Engine Status page in the right pane.



The command buttons

The command buttons in the left pane of the main administration page let you navigate to Symantec AntiVirus Scan Engine administrative functions. Clicking a command button causes the tabs for that function to appear in the right pane of the browser window.

The command buttons let you access the features in Table 3-1.

Table 3-1 Command button functions

Command button	Description
Status	Lets you examine system metrics that have been calculated since the last restart. To return to the main administration page from anywhere in the Symantec AntiVirus Scan Engine administrative interface ■ On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Status**.
Configuration	Lets you set up the Symantec AntiVirus Scan Engine for your network and configure the scan engine appropriately to provide scanning for client applications.
Blocking Policy	Lets you specify what to scan and what to block, and set limits to protect server resources.
Reporting	Lets you examine scanning statistics or log data.
LiveUpdate	Lets you update virus definitions files to ensure that your network remains protected against newly discovered viruses.
Licensing	Lets you claim new license keys and check the status of the license keys that have already been installed.
Log Off	Automatically logs you off of the administrative interface. Password reentry is required to access the interface.

The Status pane

The Status pane on the main administration page displays system metrics that are calculated since the last time that the Symantec AntiVirus Scan Engine was restarted manually (rather than restarted through the administrative interface). Metrics that are displayed in the Status pane are calculated from temporarily stored data. When the Symantec AntiVirus Scan Engine is manually shut down, the memory clears and the counts start over.

The top portion of the Status pane contains general information regarding scan engine operation. The following information displays in the top portion of the Status pane:

- Current status of the Symantec AntiVirus Scan Engine
- Version number of the Symantec AntiVirus Scan Engine that is running
- Protocol currently in use by the Symantec AntiVirus Scan Engine
- IP address and port number to which the Symantec AntiVirus Scan Engine is bound
- Date and revision number of the virus definitions that are currently in use by the Symantec AntiVirus Scan Engine
- Date and time that the scan engine was last started
- Total time that the scan engine has been running since the last restart
- The status of any license keys that have been installed

The system metrics in the bottom portion of the Status pane provide a summary of virus scanning activity since the last manual restart. To obtain more detailed data on the virus scanning activity, you must activate the desired logging capabilities and use the Reporting features of the Symantec AntiVirus Scan Engine. The following system metrics display in the bottom portion of the Status pane:

- Total viruses found
- Total viruses repaired (this number can be different than the total number of viruses found because some malicious code cannot be repaired)
- Total requests for scanning
- Total number of files that have been scanned

  The total number of files that have been scanned is not strictly a physical file count. The total includes the number of files as well as additional objects within container files that were scanned. Some containers, such as MIME-encoded messages and Microsoft Office documents, have additional embedded objects that are not files but that may be scanned depending on the files that you have selected for scanning (the extension list settings).
- Total megabytes of data scanned

You can update the system metrics on the Status pane or reset the counts to zero through the administrative interface.

To update the display at any time

- At the bottom of the page, click **Refresh**.

To reset the counts to zero at any time

- At the bottom of the page, click **Reset Statistics**.

Changing the administration settings

You can configure the administrative settings that are listed in Table 3-2 for the Symantec AntiVirus Scan Engine administrative interface and the virtual administrator account.

Table 3-2 Administration settings

Option	Description
HTTP bind address	The Symantec AntiVirus Scan Engine is managed through a Web-based interface, which is provided through a built-in HTTP server. The HTTP server binds to all interfaces by default. You can restrict administrative access to a specific interface by entering the appropriate bind address.
HTTP port number	The Web-based interface binds to a TCP/IP port number. You are prompted to provide an HTTP port number during installation, but the port number can be changed through the administrative interface.
Administrator password	The Symantec AntiVirus Scan Engine is managed using a virtual administrative account. The virtual administrative account is known only to the Symantec AntiVirus Scan Engine. It is not a system account. You are prompted to provide a password for this account at installation. The password for this account can be changed at any time through the Symantec AntiVirus Scan Engine administrative interface. Do not forget the password that you enter for this account because the virtual administrative account is the only account that can be used to manage the Symantec AntiVirus Scan Engine. If you forget the password for the virtual administrative account, you must clear the adminpassword variable in the configuration file, and then log on to the administrative interface to enter a new password (you won't need a password). See "Editing the Symantec AntiVirus Scan Engine configuration file" on page 158.

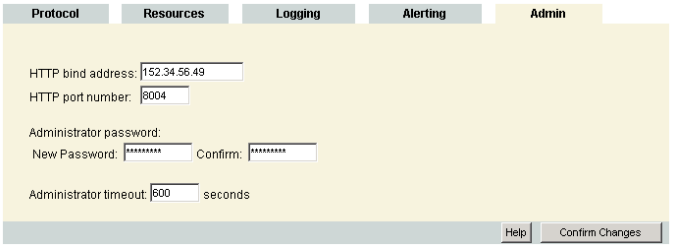
Table 3-2 Administration settings

Option	Description
Administrator timeout	The Symantec AntiVirus Scan Engine requires the administrator to log on to the administrative interface to access the administrative functions. The Symantec AntiVirus Scan Engine is configured to automatically log the administrator off after a selected period of inactivity by default. The default period of inactivity is five minutes. You can change the default timeout period.

To change the administration settings

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Admin tab, in the HTTP bind address box, type a bind address, if necessary.

   By default, the Symantec AntiVirus Scan Engine binds to all interfaces. You can restrict access to a specific interface by typing the appropriate bind address.



3. In the HTTP port number box, type a new port number.

   The default setting is port 8004. The port number must be exclusive to the Symantec AntiVirus Scan Engine interface and must not already be in use by any other program or service. Do not use port number 80. To disable the administrative interface, type a 0.
4. In the New Password box, type the new password for the virtual administrative account.
5. In the Confirm box, type the new password again to verify that you typed it correctly.
6. In the Administrator timeout box, type the period of inactivity, in seconds, after which the administrator is automatically logged off.

   The default setting is 300 seconds (5 minutes).

7 Click **Confirm Changes** to save the configuration.

8 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.

  If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the Scan Engine service now.
- Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

Chapter 4

Activating product licenses

This chapter includes the following topics:

- About licensing
- Activating a license
- Checking the license status

About licensing

Key features for the Symantec AntiVirus Scan Engine, including antivirus scanning functionality and virus definitions updates, are activated by license. Licenses are initially installed following product installation, through the Symantec AntiVirus Scan Engine administrative interface. When a license expires, for example, when a virus definitions update subscription expires, a new license must be installed to renew the subscription. When no license is installed, limited functionality is available. A license affects the relevant behavior only. For example, when no antivirus scanning license is installed, an administrator can access the administrative interface to view and modify settings and run reports, but no antivirus scanning is performed. When no virus definitions update license is installed, new virus definitions updates are not downloaded to keep protection current.

See "Activating a license" on page 53.

License warning and grace periods

When a license is within 30 days of the expiration date, it is considered to be in a warning period. After a license expires, the licensed feature continues to operate for a specified period of time. This is the grace period. If the grace period expires with no license renewal, all record of the license is removed and the product becomes unlicensed.

The Symantec AntiVirus Scan Engine can be configured to generate log entries and send alerts to indicate that a license is in the warning period or the grace period. Alerts and log entries are generated every 24 hours during the period.

See "Specifying what to log" on page 112.

See "Activating alerts" on page 77.

You can view detailed information on the status of all installed Symantec AntiVirus Scan Engine licenses at any time by clicking Licensing on the Symantec AntiVirus Scan Engine main administration page.

See "Checking the license status" on page 55.

The Symantec AntiVirus Scan Engine Status page, which is located in the left pane on the main administration page, also contains a License status entry that indicates whether any installed license is in either a grace or warning period.

Removing license files

Symantec AntiVirus Scan Engine licenses are not uninstalled automatically when the product is uninstalled. The license files remain in place, so that if you must uninstall and reinstall the Symantec AntiVirus Scan Engine for any reason, the license is intact on reinstall. Each installed license is stored in a separate file in the shared license directory that contains the licenses for all Symantec products that are activated by license. The license files must be removed manually. If you must remove a license file, contact Symantec Service and Support.

Activating a license

Both the Symantec AntiVirus Scan Engine antivirus scanning functionality and your subscription to the virus definitions updates are activated by license. A separate license must be installed for each feature. If you purchase additional product features from Symantec as they become available for the Symantec AntiVirus Scan Engine, these features will be activated with a new license.

To activate a license, you must have the serial number required for activation. The serial number is printed on the Symantec Serial Number Certificate for the product.

Note: The Symantec Serial Number Certificate is not part of the Symantec AntiVirus Scan Engine software distribution package. The Symantec Serial Number Certificate is mailed separately and should arrive in the same time frame as your software.

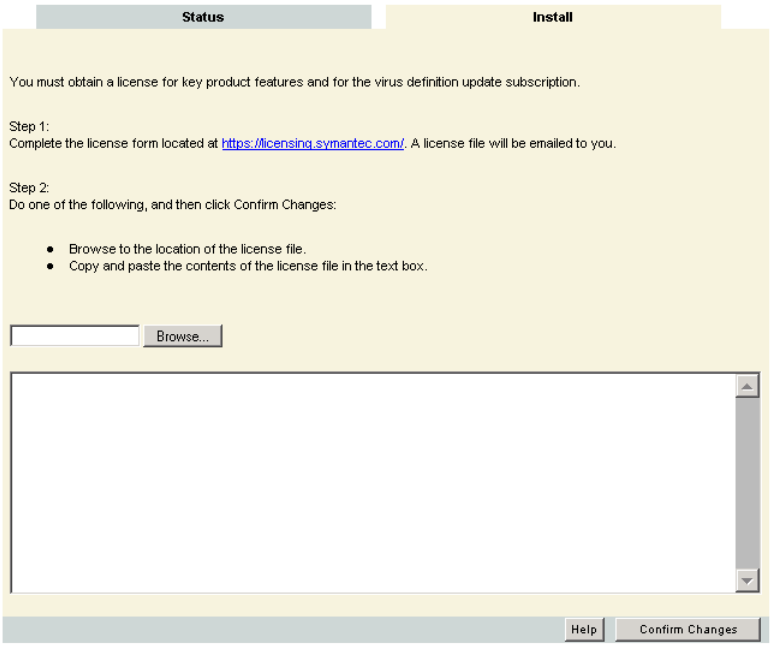
To activate a license

Activating a license is a two-step process. You must complete both steps to activate a license:

- Obtain the license file from Symantec by completing the online form. You must have a serial number to complete the online form. Once you complete the online form, you receive the license file via email from Symantec (the complete license file is provided as an attachment to the email).
- Install the license file that you receive via the Symantec AntiVirus Scan Engine administrative interface.

To obtain the license file

1 On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Licensing**.


Status
Install
You must obtain a license for key product features and for the virus definition update subscription.
Step 1:
Complete the license form located at https://licensing.symantec.com/. A license file will be emailed to you.
Step 2:
Do one of the following, and then click Confirm Changes:
Browse to the location of the license file.
Copy and paste the contents of the license file in the text box.
Browse...
Help
Confirm Changes

2 On the Install tab, click the link to access Symantec's Licensing and Registration Web page.

3 Follow the instructions on the Web page to complete the online licensing form.

You must have the appropriate serial number to complete the form.

The license file is returned via email as an attachment. Make sure that the email address you provide on the online form is appropriate so that the license file will be accessible.

To install the license file

1. When you receive the email message from Symantec that contains the license file, save the file that is attached to the email message to the computer from which you will access the Symantec AntiVirus Scan Engine administrative interface.
2. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Licensing**.
3. Do one of the following:
   - On the Install tab, click **Browse** to browse to the location of the license file.

     The path to the file should appear in the box to the left of the Browse button.
   - Open the license file using a text editor, such as Notepad, and copy and paste the entire contents of the file into the field on the Install tab.

     Make sure that you use a text editor such as Notepad to open the file. Because the license file is an XML file, browsers such as Microsoft Internet Explorer add extra code as they open the license file. If the license file is altered in any way it will not install.
4. Click **Confirm Changes**.

   The software indicates whether the license was installed successfully.
5. Click **Continue**.

   If the license was installed successfully, clicking Continue returns you to the Status tab so that you can verify the updated license status. If the license did not install, clicking Continue returns you to the Install tab so that you can attempt the installation again.

Checking the license status

You can access detailed information on the Symantec AntiVirus Scan Engine product licenses at any time by clicking Licensing on the Symantec AntiVirus Scan Engine main administration page and viewing the Status tab. For any installed license, you can check the license expiration date, the number of days remaining in the warning or grace period (if applicable), and the number of nodes licensed. A fulfillment ID for each installed license also appears on the Status tab. You will need to supply the fulfillment ID to Symantec Service and Support if you have questions regarding your license.

The license information that is displayed is described in Table 4-1.

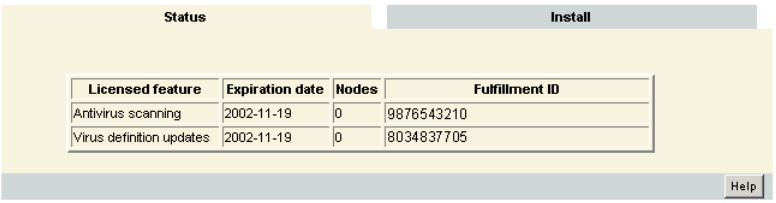
Table 4-1 License status information

Column	Description
Licensed feature	Each installed license is listed according to the feature that is activated by the license.
Expiration date	The expiration date for each license is displayed. If the license is in either the warning period or the grace period, a warning message is also displayed in this column.
Nodes	The number of licensed nodes is displayed for each installed license.
Fulfillment ID	The fulfillment ID is the identification number for your license. Provide this number to Symantec Service and Support if you have questions regarding your license.

Note: You can also check the status of your licenses from the Symantec AntiVirus Scan Engine Status page, which is located in the left pane on the main administration page. The Status page displays a License status entry that indicates whether any installed license is in either a grace or warning period. However, for more detailed information, you must click Licensing.

To check the license status

1 On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Licensing**.



2 On the Status tab, review the license information that is displayed.

Chapter 5

Configuring the Symantec AntiVirus Scan Engine

This chapter includes the following topics:

- About configuring the Symantec AntiVirus Scan Engine
- Selecting the communication protocol
- Allocating resources
- Activating alerts

About configuring the Symantec AntiVirus Scan Engine

You can set up the Symantec AntiVirus Scan Engine for your network and configure the scan engine appropriately to provide scanning services for client applications. You can do the following:

- Change the protocol that the scan engine uses to communicate with the client applications for which it is providing scanning services, and configure any protocol-specific settings.
- Allocate server and scan engine resources for operation of the Symantec AntiVirus Scan Engine.
- Activate SNMP and SMTP alerting for selected Symantec AntiVirus Scan Engine activities.

Selecting the communication protocol

You can change the communication protocol that the scan engine uses to communicate with the client applications for which it is providing scanning services.

See "About supported protocols" on page 20.

You can choose from the following protocols:

- The Symantec AntiVirus Scan Engine native protocol: The Symantec AntiVirus Scan Engine uses its own native protocol by default. The native protocol is a simple TCP/IP protocol, which is text-based like HTTP or SMTP, and uses standard ASCII commands and responses to communicate between client and server.

  See "Configuring the Symantec AntiVirus Scan Engine native protocol" on page 59.
- The Internet Content Adaptation Protocol (ICAP): ICAP is a lightweight protocol for executing a remote procedure call on HTTP messages. The Symantec AntiVirus Scan Engine supports both the proprietary 0.95 implementation of ICAP and the December 2001 draft 1.0 ICAP standard. The Symantec AntiVirus Scan Engine determines which is appropriate for the request based on the header data provided by the client application.

  See "Configuring ICAP" on page 61.

- Remote procedure call (RPC): The Symantec AntiVirus Scan Engine can be configured for Windows 2000 Server/Advanced Server to use a proprietary virus scanning protocol with the MS-RPC protocol to interface with client applications. If you are running the Symantec AntiVirus Scan Engine on Solaris or Linux, this option does not appear on the administrative interface.
  See "Configuring RPC" on page 64.

After you select a protocol, you must provide protocol-specific configuration information. The configuration options differ depending on the protocol that you select.

Configuring the Symantec AntiVirus Scan Engine native protocol

In its default configuration, the Symantec AntiVirus Scan Engine implements a simple TCP/IP protocol to provide antivirus functionality to client applications. This protocol is text-based like HTTP or SMTP, and uses standard ASCII commands and responses to communicate between client and server. To submit a file for scanning, a client connects to the specified IP port, sends the file to be scanned, and reads the results of the scan. After the scan results are received, the connection is terminated. A new connection is initiated for each file to be scanned.

If you select the native protocol, you must configure several protocol-specific options. The information in Table 5-1 must be provided when the native protocol is selected.

Table 5-1 Protocol-specific options for the native protocol

Option	Description
Scan engine bind address	By default, the Symantec AntiVirus Scan Engine binds to all interfaces. You can restrict access to a specific interface by entering the appropriate bind address. You can use 127.0.0.1 (the loopback interface) to let only clients that are running on the same computer connect to the Symantec AntiVirus Scan Engine.
Port number	The specified port number must be exclusive to the Symantec AntiVirus Scan Engine. The default port number is 7777. If you change the port number, use a number that is greater than 1024 that is not in use by any other program or service. If you are installing more than one instance of the Symantec AntiVirus Scan Engine on a single computer, each Scan Engine service must have a unique port number.

Table 5-1 Protocol-specific options for the native protocol

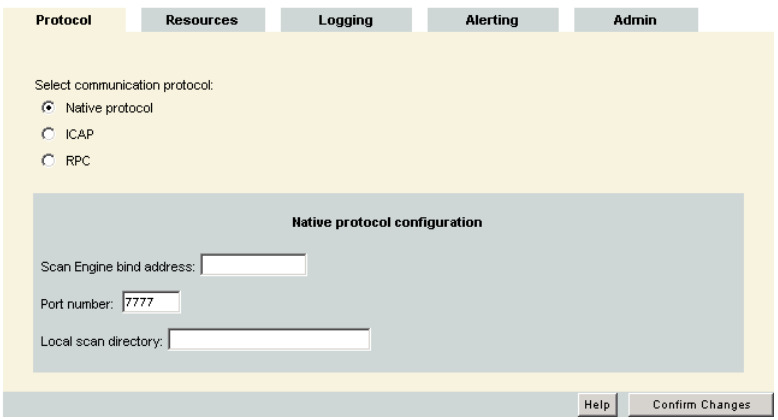
Option	Description
Local scan directory	You only need to provide a local scan directory when you are using local file scanning options (that is, the client application and the Symantec AntiVirus Scan Engine are running on the same computer and files are scanned in place on the computer) and you want to limit the Symantec AntiVirus Scan Engine so that only files under a particular directory can be scanned. If a local scan directory is not specified (this is the default), any file can be scanned. The directory that you specify must already exist.

If you are running the Symantec AntiVirus Scan Engine on Windows 2000 Server/Advanced Server and you change the protocol setting to the native protocol, you may need to change the service startup properties to identify an account that has sufficient permissions on which the Symantec AntiVirus Scan Engine will run.

See "Editing the service startup properties" on page 69.

To configure the native protocol

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Protocol tab, click **Native protocol**.
   The configuration settings display for the selected protocol.



3. In the Scan Engine bind address box, type a bind address, if necessary.

   By default, the Symantec AntiVirus Scan Engine binds to all interfaces. You can restrict access to a specific interface by typing the appropriate bind address. Use 127.0.0.1 (the loopback interface) to let only clients that are running on the same computer connect to the Symantec AntiVirus Scan Engine.

4. In the Port number box, type the TCP/IP port number to be used by client applications to pass files to the scan engine for scanning.

   The default setting is port 7777.

5. In the Local scan directory box, type a local scan directory, if necessary.

   Any file can be scanned by default (no local scan directory is specified). If you specify a directory for local scanning and you have client antivirus software installed to protect the computer that is running the Symantec AntiVirus Scan Engine, you must exclude the local scan directory from real-time scanning and from all scheduled and manually invoked scans by the client antivirus software before passing files to the Symantec AntiVirus Scan Engine for scanning.

6. Click **Confirm Changes** to save the configuration.

7. Do one of the following:

   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.

     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.

   - Click **Restart** to save your changes and restart the Scan Engine service now.

   - Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

Configuring ICAP

The Symantec AntiVirus Scan Engine can be configured to use ICAP to communicate with clients that are running either the proprietary version 0.95 or the December 2001 draft standard version 1.0 of ICAP. Any appropriate client can use ICAP to communicate with the Symantec AntiVirus Scan Engine to request the scanning and repairing of files. If you select ICAP as the protocol to be used by the Symantec AntiVirus Scan Engine, you must configure several ICAP-specific options. You must also configure the ICAP client to work with the Symantec AntiVirus Scan Engine.

You can configure multiple client applications that use different versions of ICAP to pass files to a single Symantec AntiVirus Scan Engine. When you select ICAP as the communication protocol for the scan engine, the scan engine determines the appropriate version of ICAP to use based on the header data passed in from the client application.

The protocol-specific information in Table 5-2 must be provided when ICAP is selected.

Table 5-2 Protocol-specific options for ICAP

Option	Description
Scan Engine bind address	By default, the Symantec AntiVirus Scan Engine binds to all interfaces. You can restrict access to a specific interface by entering the appropriate bind address. You can use 127.0.0.1 (the loopback interface) to let only clients that are running on the same computer connect to the Symantec AntiVirus Scan Engine.
Port number	The port number must be exclusive to the Symantec AntiVirus Scan Engine. The default port number is 1344. If you change the port number, use a number that is greater than 1024 that is not in use by any other program or service. If you are installing more than one instance of the Symantec AntiVirus Scan Engine on a single computer, each Scan Engine service must have a unique port number.
HTML message displayed for infected files	The Symantec AntiVirus Scan Engine includes a default HTML message to display to users when access to a file is denied because it contains a virus. You can customize this message by specifying an alternate path and file name or by editing the existing file. If you choose to edit the existing file, you do not have to change this setting.
ICAP scan policy	When an infected file is found, the Symantec AntiVirus Scan Engine can do any of the following: ■ Scan only: Deny access to the infected file (but do nothing to the infected file). ■ Scan and delete: Delete all infected files, including files that are embedded in archive files, without attempting repair. ■ Scan and repair files: Attempt to repair infected files (but do nothing to files that cannot be repaired). ■ Scan and repair or delete: Attempt to repair infected files, and delete any unrepairable files from archive files.

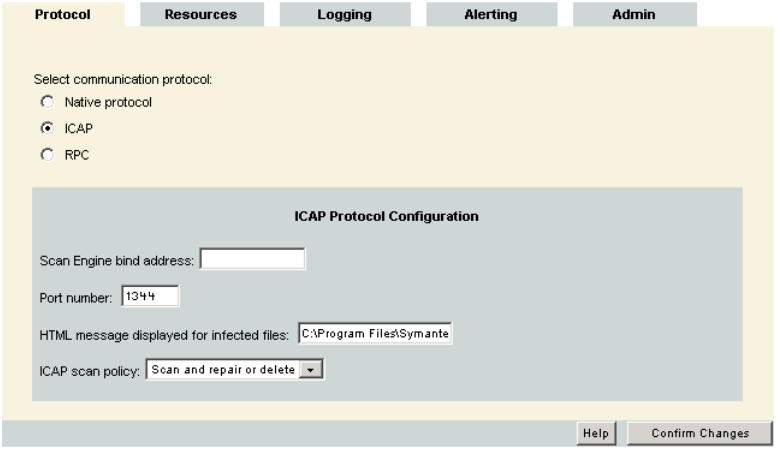
Note: If you are using ICAP 1.0, depending on the ICAP client for which the scan engine is providing scan and repair services, you may need to adjust the ICAP response from the scan engine when a file is blocked because it is infected and cannot be repaired. The default setting is to send a replacement file when an unrepairable file is blocked. However, some ICAP 1.0 applications are configured to receive an ICAP 403 response instead. You can adjust this setting by editing the configuration file.

See "Configuring ICAP via the configuration file" on page 160.

To configure ICAP

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Protocol tab, click **ICAP**.

   The configuration settings display for the selected protocol.



3. In the Scan Engine bind address box, type a bind address, if necessary.

   By default, the Symantec AntiVirus Scan Engine binds to all interfaces. You can restrict access to a specific interface by typing the appropriate bind address. Use 127.0.0.1 (the loopback interface) to let only clients that are running on the same computer connect to the Symantec AntiVirus Scan Engine.

4. In the Port number box, type the TCP/IP port number to be used by client applications to pass files to the Symantec AntiVirus Scan Engine for scanning.

   The default setting for ICAP is port 1344.

5. In the HTML message displayed for infected files box, type the path and file name to supply an alternate HTML file, if necessary.

6. In the ICAP scan policy drop-down list, select how you want the Symantec AntiVirus Scan Engine to handle infected files.

   The default setting is Scan and repair or delete.

7. Click **Confirm Changes** to save the configuration.

8. Do one of the following:

   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.

     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.

   - Click **Restart** to save your changes and restart the Scan Engine service now.

   - Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

Configuring RPC

The Symantec AntiVirus Scan Engine can be configured to use RPC to interface with appropriate clients (for Windows 2000 Server/Advanced Server). Any appropriate client application can use RPC to communicate with the Symantec AntiVirus Scan Engine and request the scanning and repairing of files. If you select RPC as the protocol to be used by the Symantec AntiVirus Scan Engine, you must configure RPC-specific settings. The RPC client also must be configured to work with the Symantec AntiVirus Scan Engine.

The protocol-specific information in Table 5-3 must be provided when the RPC protocol is selected.

Table 5-3 Protocol-specific options for RPC

Option	Description
RPC client IP addresses	A single Symantec AntiVirus Scan Engine can support one or more RPC clients. Clients must be located in the same domain as the scan engine. You must provide the IP address of each RPC client.
Check RPC connection every __ seconds	The Symantec AntiVirus Scan Engine maintains a connection with the RPC client. The Symantec AntiVirus Scan Engine can be configured to check the RPC connection with the client periodically to ensure that the connection is active. The default value is 20 seconds.
Maximum number of reconnect attempts	The Symantec AntiVirus Scan Engine can be configured to make a specified number of attempts to reestablish a lost connection with the RPC client. If the maximum number of attempts is made to reestablish the connection with no reply from the client, the Symantec AntiVirus Scan Engine shuts down. By default, the Symantec AntiVirus Scan Engine is configured to try to reconnect with the RPC client indefinitely. **Note:** Do not set a maximum number of reconnect attempts if the scan engine is providing scanning for multiple RPC clients. Use the default setting, so that the Symantec AntiVirus Scan Engine tries indefinitely to reconnect to the RPC clients.
RPC scan policy	When an infected file is found, the Symantec AntiVirus Scan Engine can do any of the following: ■ Scan only: Deny access to the infected file (but do nothing to the infected file). ■ Scan and repair files: Attempt to repair infected files and deny access to any unrepairable files. ■ Scan and repair or delete: Attempt to repair infected files, and delete any unrepairable files from archive files. **Note:** If you plan to quarantine infected files that cannot be repaired, you must select Scan and repair or delete.

If you change the protocol setting to RPC through the administrative interface (rather than uninstalling and reinstalling the scan engine), you may need to change the service startup properties to identify an account with sufficient permissions on which the Symantec AntiVirus Scan Engine will run. You may also need to change the service startup properties if you edit the list of RPC clients.

See "Editing the service startup properties" on page 69.

When you are using the RPC protocol, you can quarantine unrepairable infected files using the Symantec Central Quarantine version 3.0. The Symantec Central Quarantine software is included on the Symantec AntiVirus Scan Engine distribution CD along with supporting documentation.

See the separate Symantec Central Quarantine document (CentQuar.pdf), also included on the CD, for more information.

See "Quarantining unrepairable infected files" on page 70.

To configure RPC

To configure RPC, you must do the following:

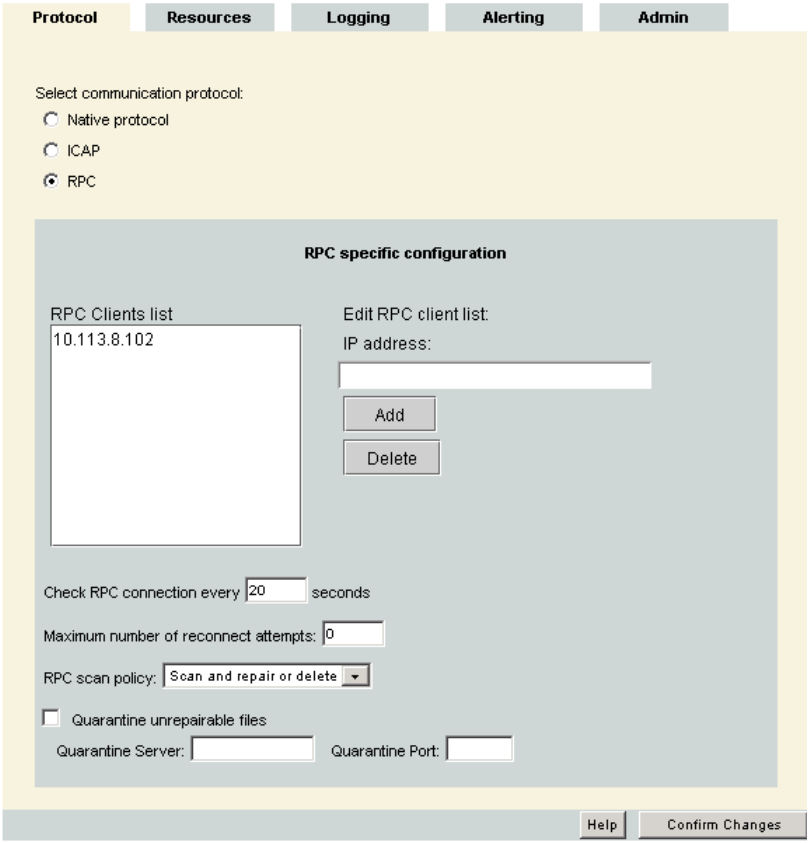
- Provide an IP address for each RPC client for which the Symantec AntiVirus Scan Engine will provide scanning services. You can add or delete RPC clients from this list at any time.
- Configure the additional RPC-specific options.

To edit the list of RPC clients

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Protocol tab, click **RPC**.
   The configuration settings are displayed for the selected protocol.
3. To add an RPC client to the list of RPC clients, do the following:
   - In the IP address box, type an IP address for an RPC client for which the Symantec AntiVirus Scan Engine will provide scanning services.
   - Click **Add**.
     The list of RPC clients updates to reflect your changes.
4. To delete an RPC client from the list of RPC clients, do the following:
   - In the list of RPC clients, select the IP address of the RPC client to be deleted.
     You can select more than one entry by pressing Enter and selecting the desired entries.
   - Click **Delete**.
5. Click **Confirm Changes** to save the configuration.
6. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
   - Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

To configure additional RPC-specific options

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Protocol tab, click **RPC**.
   The configuration settings are displayed for the selected protocol.



3. In the Check RPC connection every box, type how frequently the Symantec AntiVirus Scan Engine checks the RPC connection with the RPC client to ensure that the connection is active.
   The default interval is 20 seconds.

4. In the Maximum number of reconnect attempts box, type the maximum number of attempts that the Symantec AntiVirus Scan Engine will make to reestablish a lost connection with the RPC client.

   The default setting is 0, which causes the Symantec AntiVirus Scan Engine to try indefinitely to reestablish a connection. Use the default setting if the scan engine is providing scanning for multiple RPC clients.

5. In the RPC scan policy drop-down list, select how you want the Symantec AntiVirus Scan Engine to handle infected files.

   The default setting is Scan and repair or delete.

6. Click **Confirm Changes** to save the configuration.

7. Do one of the following:

   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.

     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.

   - Click **Restart** to save your changes and restart the Scan Engine service now.

   - Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

Editing the service startup properties

If the Symantec AntiVirus Scan Engine is installed on Windows 2000 Server/ Advanced Server and you change the protocol setting to RPC or the native protocol through the administrative interface, you may need to change the service startup properties to identify an account that has the appropriate permissions. The selected account must provide the Symantec AntiVirus Scan Engine with access to and appropriate permissions on the RPC clients (for RPC) or to any shared drives or UNC paths for which scanning services are to be provided (for the native protocol).

For RPC, this account must have Backup Operator privileges on the RPC clients. For the native protocol, this account should have access to any shared drives or UNC paths for which scanning is to be provided and should have Change permission if infected files that cannot be repaired are to be deleted.

Note: If you select RPC at installation, you are prompted to enter the account name and password for this account as part of the installation process and do not need to edit the service startup properties manually. This step is only necessary if you change protocols after installation through the administrative interface (rather than uninstalling and reinstalling).

To edit the service startup properties for Windows 2000 Server/Advanced Server

1. In the Windows 2000 Control Panel, click **Administrative Tools**.
2. Click **Services**.

   Two Symantec AntiVirus Scan Engine services are listed: Symantec AntiVirus Scan Engine Watchdog, which monitors the Symantec AntiVirus Scan Engine to ensure that it is always running, and Symantec AntiVirus Scan Engine.
3. Right-click **Symantec AntiVirus Scan Engine**, then click **Properties**.
4. In the Properties dialog box, on the Log On tab, click **This Account**.
5. Type the account name and password for the account on which the Symantec AntiVirus Scan Engine will run.

   Use the following format for the account name: domain\username.
6. Click **OK**.
7. Stop and restart the Symantec AntiVirus Scan Engine service.

Quarantining unrepairable infected files

When you are using the RPC protocol, you can quarantine unrepairable infected files. Quarantining of infected files is handled using the separately installed Symantec Central Quarantine version 3.0.

The Symantec AntiVirus Scan Engine forwards infected items that cannot be repaired to the Symantec Central Quarantine. Typically, heuristically detected viruses that cannot be eliminated by the current set of virus definitions are forwarded to the Quarantine and isolated so that the viruses cannot spread. From the Quarantine, the infected items can be submitted to Symantec Security

Response for analysis. If a new virus is identified, new virus definitions are posted.

Note: You must select Scan and repair or delete as the RPC scan policy to forward files to the Quarantine. Once a copy of an infected file is forwarded to the Central Quarantine, the original infected file is deleted. If submission to the Central Quarantine is not successful, the original file is not deleted, and an error message is returned to the RPC client. In this case, access to the infected file is denied.

The Symantec Central Quarantine is installed separately. It must be installed on a computer that is running Windows 2000 Server/Advanced Server in accordance with the supporting documentation. The Symantec Central Quarantine software and supporting documentation is included on the Symantec AntiVirus Scan Engine distribution CD.

See the separate Symantec Central Quarantine document (CentQuar.pdf) for more information.

If you plan to quarantine infected files that cannot be repaired, you must configure the Symantec AntiVirus Scan Engine to quarantine infected files and provide information for contacting the Symantec Quarantine Server.

To quarantine unrepairable infected files

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Protocol tab, under RPC specific configuration, check **Quarantine unrepairable files**.
3. In the Quarantine Server box, type the host name or the IP address for the computer on which the Symantec Quarantine Server is installed.
4. In the Quarantine Port box, type the TCP/IP port number to be used by the Symantec AntiVirus Scan Engine to pass files to the Central Quarantine.

   This setting must match the port number that is selected at installation for the Symantec Quarantine Server.

5 Click **Confirm Changes** to save the configuration.

6 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.

  If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the Scan Engine service now.
- Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

Allocating resources

You can allocate resources for the operation of the Symantec AntiVirus Scan Engine. You can specify the settings that are listed in Table 5-4.

Table 5-4 Resource settings

Option	Description
Temporary directory for virus scanning	The Symantec AntiVirus Scan Engine stores files in a temporary directory for virus scanning. To support sites with large, specialized disk configuration, the location of this temporary directory can be specified. The disk space that is required for this directory varies depending on the volume of files to be scanned. Scan engine performance is dependent on this directory being able to accommodate potentially large numbers of large files during periods of peak usage. The default temporary directory for Linux and Solaris is /tmp/navtemp. The default temporary directory for Windows 2000 Server/Advanced Server is determined at installation. The temporary directory for the Symantec AntiVirus Scan Engine defaults to the temporary directory that is set for one of the following environment variables (listed in the order in which they are checked): ■ System tmp ■ System temp ■ User tmp (the user that is performing the installation) ■ User temp (the user that is performing the installation) If none of these has a temporary directory assigned, the temporary directory is the installation directory.

Table 5-4 Resource settings

Option	Description
Number of available threads for scanning	You can select the number of threads that are available for concurrent scanning. Usage may be the only method for determining the optimal setting for the number of available threads. Scan engine performance is dependent on scan volume, the number of client applications making requests, available memory and disk space, and the selected number of scanning threads. **Note:** When the number of scan requests exceeds the number of scanning threads that are available, scan requests are queued until a thread becomes available. The threshold number of queued requests is configurable for the Symantec AntiVirus Scan Engine. **Note:** If you are using the RPC protocol and are supporting multiple RPC clients, the Symantec AntiVirus Scan Engine creates a separate pool of threads for each RPC client (the RPC clients do not share a common pool of threads). Thus, the number of available threads for scanning that you select for this setting is applied to each RPC client individually.
Threshold number of queued requests	When the number of queued requests to the Symantec AntiVirus Scan Engine exceeds the specified threshold, the scan engine is at maximum load. The Symantec AntiVirus Scan Engine can be configured to log periods of time when it is at maximum load and to generate Load Exceeded alerts at a prescribed interval. **Note:** The Symantec AntiVirus Scan Engine continues to queue all incoming requests after the threshold is exceeded.
Log or send alerts for maximum load every __ minutes	The alert interval is the number of minutes between log entries or alerts generated to indicate that maximum load has been exceeded. Maximum load is exceeded when the number of requests to the Symantec AntiVirus Scan Engine exceeds the specified threshold number of queued requests. If you change the alert interval, the Symantec AntiVirus Scan Engine may remain at maximum load for a period of time. Select an interval that will be informative but will not result in an excessive amount of alert messages or log entries during that period. **Note:** For logging or alerting to occur when the scan engine is at maximum load, you must activate logging/alerting for threshold number of queued requests exceeded. See "Configuring standard logging" on page 111 and "Activating alerts" on page 77.

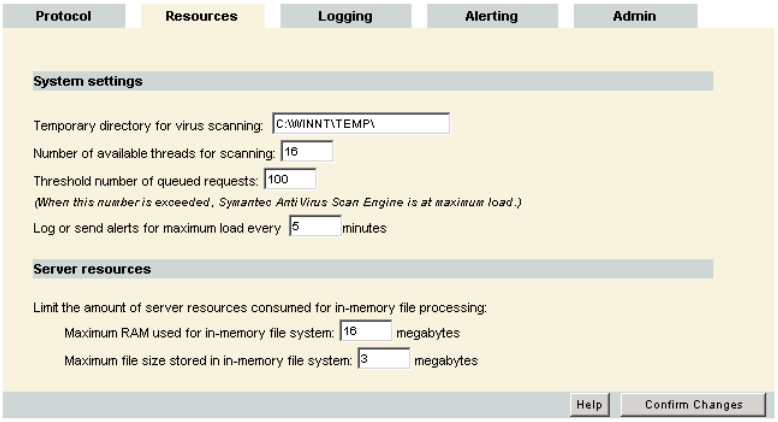
Table 5-4 Resource settings

Option	Description
Virus definition product name	Solaris and Linux permit multiple instances of the Symantec AntiVirus Scan Engine on the same computer. If you are running more than one scan engine on a single computer, the product name must be unique for each Scan Engine service so that both scan engines receive updated virus definitions via LiveUpdate. This option only appears if you are running the scan engine on Solaris or Linux.
In-memory file processing limits	The Symantec AntiVirus Scan Engine can decompose and scan the contents of container files in memory, which eliminates the latency imposed by on-disk scanning. This feature can improve performance in environments in which large volumes of container and archive file formats are routinely submitted for scanning. You can limit the resources consumed for in-memory file processing by specifying the following: ■ The maximum amount of RAM (in megabytes) used for the in-memory file system ■ The maximum file size (in megabytes) that can be stored in the in-memory file system

To allocate resources for the Symantec AntiVirus Scan Engine

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Resources tab, under System settings, type the temporary directory to be used for virus scanning.

   If you have client antivirus software installed to protect the computer that is running the Symantec AntiVirus Scan Engine, you must exclude the temporary directory from real-time scanning and from all scheduled and manually invoked scans by the client antivirus software before passing files to the Symantec AntiVirus Scan Engine for scanning.


Protocol
Resources
Logging
Alerting
Admin
System settings
Temporary directory for virus scanning: C:\WINNT\TEMP\
Number of available threads for scanning: 16
Threshold number of queued requests: 100
(When this number is exceeded, Symantec AntiVirus Scan Engine is at maximum load.)
Log or send alerts for maximum load every 5 minutes
Server resources
Limit the amount of server resources consumed for in-memory file processing:
Maximum RAM used for in-memory file system: 16 megabytes
Maximum file size stored in in-memory file system: 3 megabytes
Help
Confirm Changes

3. In the Number of available threads for scanning box, type the number of scanning threads that are available for concurrent scanning.

   The default number of threads is 16. Use the information in Table 5-5 as a guide for determining the number of scanning threads.

Table 5-5 Performance metrics for determining the number of available scanning threads

	Sun Ultra 10	Sun Ultra 10	Sun Ultra 60	Sun Ultra 60
Number of scan threads	20	20	10	20
Files per second	16	26	43	46
Simultaneous clients	20	30	100	100
CPU utilization (percent)	40%	60%	61%	68%

Table 5-5 Performance metrics for determining the number of available scanning threads

	Sun Ultra 10	Sun Ultra 10	Sun Ultra 60	Sun Ultra 60
Average processing time per file (seconds)	0.48	0.36	1.41	0.53
Files scanned in under 1 second (percent)	98%	99%	98.794%	97.3828%
Files scanned in under 10 seconds (percent)	100%	100%	99.918%	99.8765%

4. In the Threshold number of queued requests box, type the threshold number of queued requests above which the Symantec AntiVirus Scan Engine is considered to be at maximum load.

   The default setting is 100.

5. If you have chosen to log or generate alerts when maximum load is exceeded, in the Log or send alerts for maximum load every box, type the desired alert interval in minutes.

   The default setting is five minutes.

6. If you are running more than one instance of the Symantec AntiVirus Scan Engine on Solaris or Linux, under Advanced settings, type an alternate virus definition product name in the box provided.

   The default is SCANENGINE_40. If you are running the Symantec AntiVirus Scan Engine on Windows 2000 Server/Advanced Server, this setting does not appear on the administrative interface.

7. Under Server resources, in the Maximum RAM used for in-memory file system box, type the maximum amount of RAM that can be used for the in-memory file system.

   The default setting is 16 megabytes.

8. In the Maximum file size stored in in-memory file system box, type the maximum file size that can be stored in the in-memory file system.

   The default setting is 3 MB. Files that exceed the specified size are written to disk.

9 Click **Confirm Changes** to save the configuration.

10 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.

  If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the Scan Engine service now.
- Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

Activating alerts

The Symantec AntiVirus Scan Engine provides SMTP (simple mail transfer protocol) and SNMP (simple network management protocol) alerting capabilities, including startup, shutdown, virus definitions updates, infections found, and so on. You can activate SNMP and SMTP alerting individually by providing the necessary information for the delivery of the alerts. Once you have provided this information, you select the specific events on which to generate alerts.

To activate SNMP alerting, you must provide the SNMP community string and the IP address for a primary SNMP console for receiving the alerts. A second SNMP console can be identified if one is available. Alerts are sent to both the primary and secondary SNMP consoles in all cases.

See "Activating SNMP alerting" on page 77.

To activate SMTP alerting, you must identify a primary SMTP server for forwarding alert messages. You must also specify the email addresses of the recipients and the local domain for the Symantec AntiVirus Scan Engine. A second SMTP server also can be identified if one is available.

See "Activating SMTP alerting" on page 80.

Activating SNMP alerting

To activate SNMP alerting, you must provide the SNMP community string and an IP address for a primary SNMP console for receiving the alerts. You can specify a second SNMP console if one is available. Alerts are sent to both the primary and secondary SNMP consoles in all cases.

If you need the Management Information Base file to configure SNMP alerting, the file (symcscan.mib) is located in the MIB directory as part of the Symantec AntiVirus Scan Engine distribution.

You select the specific events that will generate SNMP alerts. The events are described in Table 5-6.

Table 5-6 Events for SNMP alerts

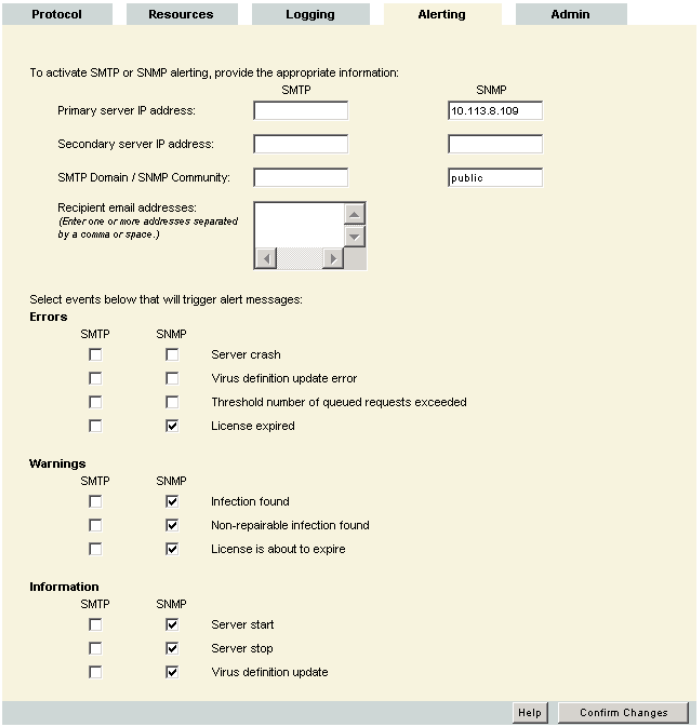
Event	SNMP alert description
Server crash	Sends SNMP alerts for all instances of scan engine crashes
Virus definition update error	Sends SNMP alerts for all errors that occur in virus definitions updates
Threshold number of queued requests exceeded	Sends SNMP alerts (at the configured alert interval) for periods of time when the maximum load is exceeded for the Symantec AntiVirus Scan Engine
License expired	Sends SNMP alerts every 24 hours when a Symantec AntiVirus Scan Engine license has expired **Note:** License expired alerts are generated only during the grace period following the license expiration date. If the grace period expires before the license is renewed, all record of the license is removed and the product or feature becomes unlicensed.
Infection found	Sends SNMP alerts for all infections found (regardless of whether the infected file is repairable or nonrepairable)
Non-repairable infection found	Sends an SNMP alert only when an infection is found and the file cannot be repaired **Note:** When the Symantec AntiVirus Scan Engine is set to Scan Only, this alert is generated for any infection that is found.
License about to expire	Sends SNMP alerts every 24 hours when a Symantec AntiVirus Scan Engine license is about to expire (that is, the license is within 30 days of its expiration date)

Table 5-6 Events for SNMP alerts

Event	SNMP alert description
Server start	Sends SNMP alerts for all instances of scan engine startup
Server stop	Sends SNMP alerts for all instances of scan engine shutdown
Virus definition update	Sends SNMP alerts for all instances of scan engine virus definitions updates

To activate SNMP alerting for the Symantec AntiVirus Scan Engine

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Alerting tab, in the Primary server IP address box, under SNMP, type the IP address of the primary SNMP console to receive alerts.



3. In the Secondary server IP address box, under SNMP, type the IP address of a secondary SNMP console to receive alerts if one is available.
4. In the SMTP Domain/SNMP Community box, under SNMP, type the SNMP community string.
   The default setting is public.
5. Under Select events below that will trigger alert messages, check the individual events for which SNMP alerts will be generated.
6. Click **Confirm Changes** to save the configuration.
7. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
   - Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

Activating SMTP alerting

To activate SMTP alerting, you must identify a primary SMTP server for forwarding alert messages. You must also specify the email addresses of the recipients and the local domain for the Symantec AntiVirus Scan Engine. You also can specify a second SMTP server if one is available.

You can select the specific events that will generate SMTP alerts. The events are described in Table 5-7.

Table 5-7 Events for SMTP alerts

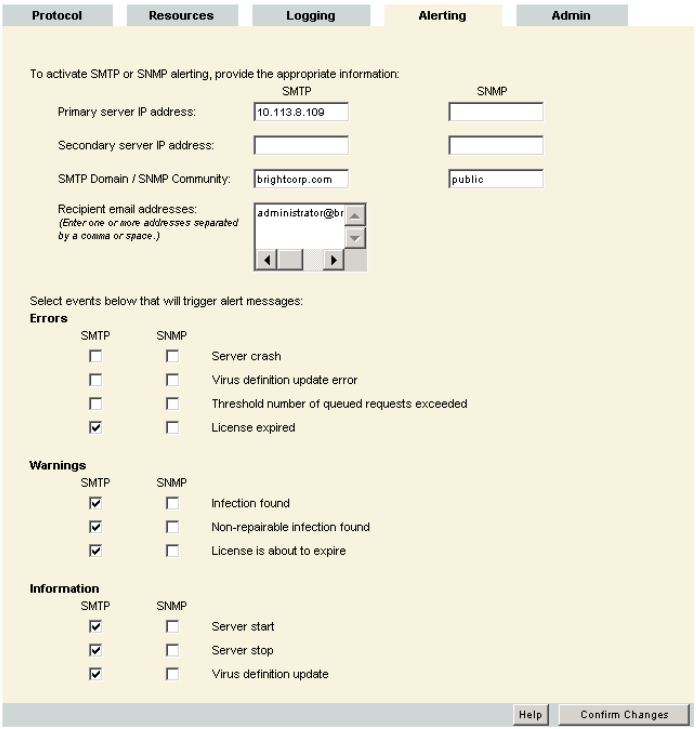
Event	SMTP alert description
Server crash	Sends SMTP alerts for all instances of scan engine crashes
Virus definition update error	Sends SMTP alerts for all errors that occur in virus definitions updates

Table 5-7 Events for SMTP alerts

Event	SMTP alert description
Threshold number of queued requests exceeded	Sends SMTP alerts (at the configured alert interval) for periods of time when the maximum load is exceeded for the Symantec AntiVirus Scan Engine
License expired	Sends SMTP alerts every 24 hours when a Symantec AntiVirus Scan Engine license has expired **Note:** License expired alerts are generated only during the grace period following the license expiration date. If the grace period expires before the license is renewed, all record of the license is removed and the product or feature becomes unlicensed.
Infection found	Sends SMTP alerts for all infections found (regardless of whether the infected file is repairable or nonrepairable) **Note:** Loss of connectivity to the SMTP server may affect scanning performance if the SMTP Infection found alert is enabled and viruses are encountered.
Non-repairable infection found	Sends an SMTP alert only when an infection is found and the file cannot be repaired **Note:** When the Symantec AntiVirus Scan Engine is set to Scan Only, this alert is generated for any infection found.
License about to expire	Sends SMTP alerts every 24 hours when a Symantec AntiVirus Scan Engine license is about to expire (that is, the license is within 30 days of its expiration date)
Server start	Sends SMTP alerts for all instances of scan engine startup
Server stop	Sends SMTP alerts for all instances of scan engine shutdown
Virus definition update	Sends SMTP alerts for all instances of scan engine virus definitions updates

To activate SMTP alerting for the Symantec AntiVirus Scan Engine

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Alerting tab, in the Primary server IP address box, under SMTP, type the IP address of the primary SMTP server that will forward the alert messages.



3. In the Secondary server IP address box, under SMTP, type the IP address of a secondary SMTP server (if one is available) that will forward the alert messages if communication with the primary SMTP server fails.
4. In the SMTP Domain/SNMP Community box, under SMTP, type the local domain for the Symantec AntiVirus Scan Engine.

   The domain name is added to the From field for SMTP alert messages so that SMTP alert messages that are generated by the Symantec AntiVirus Scan Engine originate from ScanServer@<servername>.<domainname>, where <servername> is the name of the computer that is running the Symantec AntiVirus Scan Engine and <domainname> is the domain name that is supplied here.

5 In the Recipient email addresses box, type the email addresses of the recipients of the SMTP alerts.

   Separate each email address with a comma or space.

6 Under Select events below that will trigger alert messages, check the individual events for which SMTP alerts will be generated.

7 Click **Confirm Changes** to save the configuration.

8 Do one of the following:

   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.

     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
   - Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

Chapter 6

Setting scanning and blocking policies

This chapter includes the following topics:

- About scanning and blocking policies
- Specifying processing limits
- Configuring antivirus settings
- Establishing a mail filter policy

About scanning and blocking policies

You can establish scanning and blocking policies for the Symantec AntiVirus Scan Engine. Some scanning and blocking policy features differ depending on the protocol that you are using.

Depending on a number of factors, such as scan volume, the number of client applications making requests, available memory and disk space, and the selected number of scanning threads, you may need to impose restrictions on resources to maximize performance and security. Settings that provide maximum security also consume more resources. You can configure settings to restrict the amount of resources that handle certain types of files, adjust the sensitivity of heuristic virus detection, and specify the file types to be scanned.

You can establish a blocking policy to further limit the handling and scanning of certain files. Files that meet the established criteria are blocked immediately, which limits the resources that are expended by the Symantec AntiVirus Scan Engine. For example, you can specify a maximum file name length, so that files that exceed the established limit are automatically rejected. If the Symantec AntiVirus Scan Engine is providing scanning services for email client applications, you can establish a mail policy to filter email and email attachments based on a number of attributes. (The mail policy settings are applied to all MIME-encoded messages, and do not affect nonMIME-encoded file types.)

Note: You can use some scanning and blocking policy settings during a virus outbreak to further protect your network. Once you have information on the characteristics of a new virus, you can use this information to block the infected attachment or email immediately, before virus definitions for the new virus have been posted. Or you can scan all file types rather than limiting the file types that are scanned for viruses for maximum coverage.

Specifying processing limits

You can impose restrictions on the amount of resources that can be used to handle individual files. These processing limits can be used to help you manage your resources and to protect your network against denial of service attacks.

You can specify processing limits that apply to the following:

- Large container files: The Symantec AntiVirus Scan Engine uses a decomposer to extract all of the embedded files from a container file, scan all of the files, and reassemble the container file once scanning is complete. For particularly large container files, this process can tie up a significant amount of resources. You can set limits to control the resources expended on large container files.

  See "Specifying limits for container files" on page 87.

- All files: Other types of limits can be applied to all files, such as the maximum number of bytes to be read in determining whether a file is MIME-encoded.

  See "Specifying processing limits that apply to all files" on page 90.

Specifying limits for container files

Certain container files (specifically container files that are large, that contain large numbers of embedded compressed files, or that have been designed to maliciously use resources and degrade performance) can cause a denial of service attack. To protect against these types of files, limits can be imposed on the Symantec AntiVirus Scan Engine decomposer for handling container files.

You can specify the following:

- The maximum amount of time, in seconds, that is spent decomposing a container file and its contents
- The maximum file size, in bytes, for individual files in a container file
- The maximum number of nested levels to be decomposed for scanning

You can use some or all of these limits to control how the Symantec AntiVirus Scan Engine handles container files. When any of these maximum values is met or exceeded for a given file, the Symantec AntiVirus Scan Engine stops processing the file and generates a log entry. You can specify whether to allow or deny access to files for which an established limit has been met or exceeded and for which processing has stopped. Access is denied by default.

Warning: If you plan to allow access to files for which a container violation has occurred, keep in mind that when a limit is met or exceeded, the Symantec AntiVirus Scan Engine stops processing the file, and antivirus scanning is not completed. Allowing access to a file that has not been fully scanned can potentially expose your network to viruses and other malicious content.

If you allow access to files for which a container limit violation has occurred and the scan engine finds a virus before processing stops, the scan engine will not repair the file, even if under normal circumstances the infection could be repaired. In this case, the file is handled as though the infection is unrepairable.

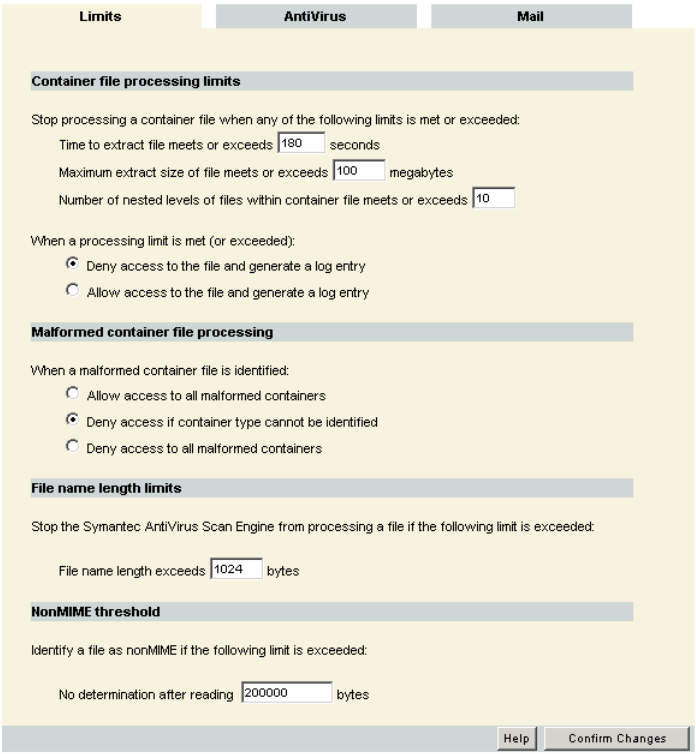
In addition to establishing resource limits for container files, you can block access to all or certain types of malformed container files. Computer viruses and malicious programs sometimes create intentionally malformed files. These distortions are recognized by the scan engine. If the scan engine can identify the container type, in many cases the scan engine can repair the container file. In other cases, the container type cannot be determined and the distortion can be used as criteria to reject potentially infected files. You can choose to allow access to all malformed containers, block only those for which the container type cannot be identified, or block access to all malformed containers. The scan engine is configured by default to block only those containers for which the container type cannot be identified.

To specify limits for container files

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the Limits tab, under Container file processing limits, in the Time to extract file meets or exceeds box, type the maximum time that the scan engine can spend extracting a single container file.

   The default setting is 180 seconds (3 minutes). To disable this setting (so that no limit is imposed), type **0**.

   Note: This setting does not apply to .hqx and .amg files.


Limits
AntiVirus
Mail
Container file processing limits
Stop processing a container file when any of the following limits is met or exceeded:
Time to extract file meets or exceeds 180 seconds
Maximum extract size of file meets or exceeds 100 megabytes
Number of nested levels of files within container file meets or exceeds 10
When a processing limit is met (or exceeded):
Deny access to the file and generate a log entry
Allow access to the file and generate a log entry
Malformed container file processing
When a malformed container file is identified:
Allow access to all malformed containers
Deny access if container type cannot be identified
Deny access to all malformed containers
File name length limits
Stop the Symantec AntiVirus Scan Engine from processing a file if the following limit is exceeded:
File name length exceeds 1024 bytes
NonMIME threshold
Identify a file as nonMIME if the following limit is exceeded:
No determination after reading 200000 bytes
Help
Confirm Changes

3. In the Maximum extract size of the file meets or exceeds box, type the maximum file size, in bytes, for individual files in a container file.

   The default setting is 100 MB. To disable this setting (so that no limit is imposed), type **0**.

4. In the Number of nested levels of files within container file meets or exceeds box, type the maximum number of nested levels of files that are decomposed within a container file.

   The default setting is 10 levels. To disable this setting (so that no limit is imposed), type **0**.

5. Select whether to allow or deny access to container files for which one or more limits are exceeded.

   Access is denied by default.

6. Under Malformed container file processing, select one of the following to specify how the scan engine handles malformed container files:

   - Allow access to all malformed containers
   - Deny access if container type cannot be identified

     This is the default setting.
   - Deny access to all malformed containers

7. Click **Confirm Changes** to save the configuration.

8. Do one of the following:

   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.

     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
   - Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

Specifying processing limits that apply to all files

You can specify the following processing limits to apply to all files (rather than just to container files):

- The maximum file name length, in bytes, for a given file (this feature is available for the native protocol only)
- The maximum number of bytes that are read when determining whether a file is MIME-encoded

To specify limits for all files

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the Limits tab, under File name length limits, in the File name length exceeds box, type the maximum file name length, in bytes, for a file name.

   The default setting is 1024 bytes. To disable this setting (so that no limit is imposed), type **0**. This feature is available for the native protocol only.
3. Under NonMIME threshold, in the No determination after reading box, type the maximum number of bytes that are read by the scan engine to determine whether a file is MIME-encoded.

   The default setting is 200000 bytes. If the Symantec AntiVirus Scan Engine reads the maximum number of bytes with no determination, the file is considered to be nonMIME-encoded.
4. Click **Confirm Changes** to save the configuration.
5. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.

     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
   - Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

Configuring antivirus settings

You can configure certain aspects of antivirus scanning, including specifying the file types to be scanned. You can change the following settings:

- Bloodhound sensitivity level: To supplement the detection of virus infections by virus signature, the Symantec AntiVirus Scan Engine includes the Symantec patented Bloodhound technology, which heuristically detects new or unknown viruses based on characteristics generally exhibited by viruses. The sensitivity of the Bloodhound technology can be adjusted.
  See "Changing the Bloodhound sensitivity level" on page 92.
- File types to scan: Viruses are found only in file types that contain executable code. Bandwidth and time can be saved by limiting the files to be scanned to only those file types that can contain viruses. You can control which file types are scanned by specifying the file extensions that you want to scan (using an inclusion list) or by specifying those extensions that you do not want to scan (using an exclusion list), or you can scan all file types regardless of extension.
  See "Specifying file types to scan" on page 93.

Changing the Bloodhound sensitivity level

The Symantec AntiVirus Scan Engine includes the Symantec patented Bloodhound technology, which heuristically detects new or unknown viruses. The sensitivity of the Bloodhound technology can be adjusted.

Note: Increasing the Bloodhound sensitivity level may lead to occasional false positives.

For more information on Symantec AntiVirus Scan Engine virus detection capabilities, see "How viruses are detected" on page 23.

To change the Bloodhound sensitivity level

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the AntiVirus tab, under Heuristic scanning, select the Bloodhound sensitivity level.

   The default Bloodhound sensitivity setting is Medium. You can select from low to high sensitivity, or you can turn off heuristic detection.
3. Click **Confirm Changes** to save the configuration.
4. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.

     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
   - Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

Specifying file types to scan

You can control which file types are scanned by specifying extensions that you do not want to scan (using an exclusion list) or by specifying extensions that you want to scan (using an inclusion list), or you can scan all file types regardless of extension. Inclusion and exclusion lists by definition do not scan all file types; thus, new types of viruses may not always be detected. Scanning all files regardless of extension is the most secure setting, but imposes the heaviest demand on resources.

Note: During virus outbreaks, you may want to scan all files even if you normally control the file types that are scanned with the inclusion or exclusion list.

The Symantec AntiVirus Scan Engine is configured by default to scan all files except those with extensions listed in a prepopulated exclusion list. The default exclusion list contains those file types that are unlikely to contain viruses, but you can edit this list.

Using an inclusion list to control which types of files are scanned is the least secure setting. Only those files types that are specifically listed in an inclusion list are scanned; thus, with an inclusion list, there is an almost limitless number of

possible file extensions that are not scanned. For this reason, the inclusion list is not prepopulated, but you can choose to populate this list if you want to limit the file types that are scanned using an inclusion list.

If you use either the inclusion or the exclusion list to control the file types that are scanned (rather than scanning all files), the manner in which the list is applied differs depending on which of the following protocols are in use by the Symantec AntiVirus Scan Engine:

- Native protocol, RPC, and ICAP version 1.0: The inclusion or exclusion list is used by the Symantec AntiVirus Scan Engine only to determine which files to scan of those that are embedded in archival file formats (for example, .zip or .lzh files). All top-level files that are sent to the Symantec AntiVirus Scan Engine are scanned regardless of file extension.

  Note: If you are using the native protocol, RPC, or ICAP version 1.0 and want to control the file types that are scanned at the top level, you must provide logic or take advantage of existing mechanisms on the client side to send only certain file types to the Symantec AntiVirus Scan Engine for scanning. The logic on the client side controls the types of files that are scanned at the top level, and the extension list setting controls which embedded files are scanned.

- ICAP version 0.95: The inclusion or exclusion list applies to all files that are sent to the Symantec AntiVirus Scan Engine for scanning. The extension list is consulted for both top-level files and embedded files that are contained in archival file formats (for example, .zip or .lzh files).

To specify which file types to scan

You can scan all files regardless of extension, or you can control which file types are scanned by specifying extensions that you do not want to scan or that you want to scan. The Symantec AntiVirus Scan Engine is configured by default to scan all files except those with extensions listed in the prepopulated exclusion list.

To scan all files regardless of extension

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the AntiVirus tab, under File types to be scanned, click **Scan all files regardless of extension**.

3 Click **Confirm Changes** to save the configuration.

4 Do one of the following:

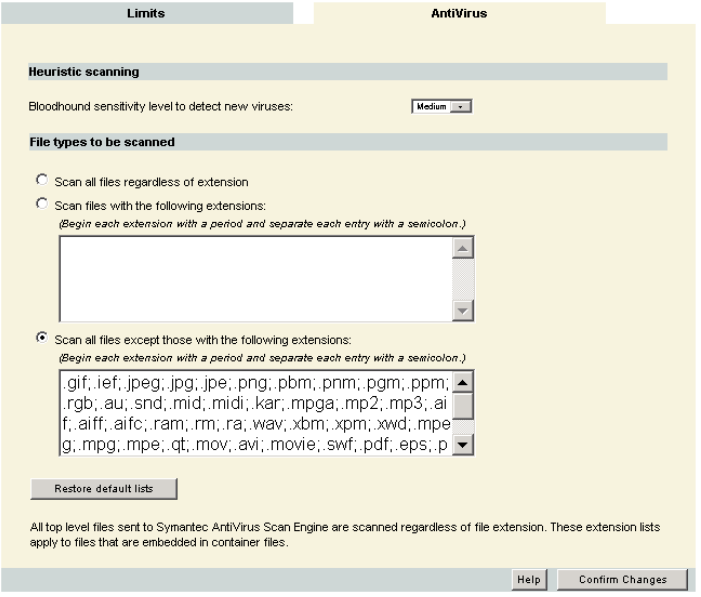
- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.

  If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the Scan Engine service now.
- Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

To scan all files except for those with extensions that are in the exclusion list

1 On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.

2 On the AntiVirus tab, under File types to be scanned, click **Scan all files except those with the following extensions**.


Limits
AntiVirus
Heuristic scanning
Bloodhound sensitivity level to detect new viruses:
Medium
File types to be scanned
Scan all files regardless of extension
Scan files with the following extensions:
(Begin each extension with a period and separate each entry with a semicolon.)
Scan all files except those with the following extensions:
(Begin each extension with a period and separate each entry with a semicolon.)
.gif;.ief;.jpeg;.jpg;.jpe;.png;.pbm;.pnm;.pgm;.ppm;
.rgb;.au;.snd;.mid;.midi;.kar;.mpga;.mp2;.mp3;.ai
f;.aiff;.aifc;.ram;.rm;.ra;.wav;.xbm;.xpm;.xwd;.mpe
g;.mpg;.mpe;.qt;.mov;.avi;.movie;.swf;.pdf;.eps;.p
Restore default lists
All top level files sent to Symantec AntiVirus Scan Engine are scanned regardless of file extension. These extension lists apply to files that are embedded in container files.
Help
Confirm Changes

3. Edit the exclusion list to add extensions that you do not want to scan or delete extensions that you want to scan.

   Use a period with each extension in the list. Separate each extension with a semicolon (for example, .com;.doc;.bat;.foo). To exclude files with no extension, use two adjacent semicolons (for example, .com;.exe;;).

4. To restore the default extension list, click **Restore default lists**.
5. Click **Confirm Changes** to save the configuration.
6. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.

     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
   - Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

To scan only files with extensions that are in the inclusion list

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the AntiVirus tab, under File types to be scanned, click **Scan files with the following extensions**.
3. Edit the inclusion list to add extensions that you want to scan or delete extensions that you do not want to scan.

   The inclusion list is blank by default. Use a period with each extension in the list. Separate each extension with a semicolon (for example, .com;.doc;.bat;.foo). To scan files that have no extensions, use two adjacent semicolons (for example, .com;.exe;;).

4 Click **Confirm Changes** to save the configuration.

5 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.

  If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the Scan Engine service now.
- Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

Establishing a mail filter policy

If the Symantec AntiVirus Scan Engine is providing scanning services for email client applications, you can establish a mail policy to filter mail and mail attachments based on a number of attributes. These mail policy settings are applied to all MIME-encoded messages.

See "Mail filter policy settings" on page 98.

Note: The mail filter policy settings are not available if you are using the RPC protocol.

Mail policy settings do not affect nonMIME-encoded file types that may be passed to the Symantec AntiVirus Scan Engine for scanning. When a mail filter policy is in effect, the mail filter settings, including the updating of mail messages to indicate that a virus has been found, are applied only to MIME-encoded messages.

You can add text to the body of MIME-encoded messages to warn recipients that a virus was found in an attachment or that an attachment was deleted because it violated the mail filter policy. The default text indicates that an attachment was infected and repaired, or deleted because it could not be repaired, or that an attachment was deleted due to a mail policy violation. Variables can be used to include the file names of the affected attachments. You can customize the text that is added by editing the Symantec AntiVirus Scan Engine message string file, symcsmsg.dat.

See "Inserting text into MIME-encoded messages" on page 107.

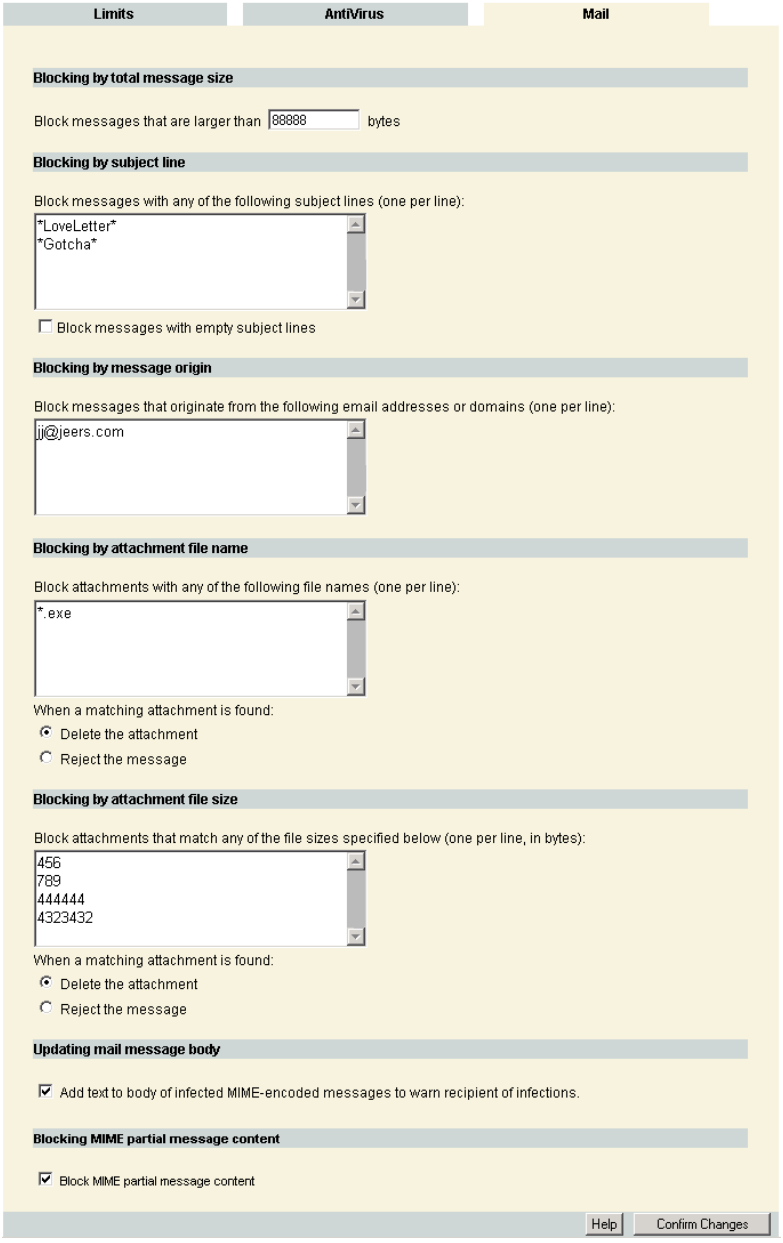
Mail filter policy settings

You can use the mail policy settings to impose general restrictions on email. You can also use some mail filters during a virus outbreak to further protect your network. For example, once you have information on the characteristics of a new virus, you can use this information to block the infected attachment or email. You can use the file name or file size option if you know the exact name or size of an infected attachment. This lets you protect your network immediately, before virus definitions for the new virus have been posted.

You can filter mail based on the settings in Table 6-1.

Table 6-1 Mail filter settings

Filtering option	Description
Total message size	Specify a maximum size for messages so that messages that exceed the maximum mail size are rejected. See "Filtering mail by total message size" on page 100.
Subject line	Specify one or more subject lines that are known to be threats so that messages with these subject lines are rejected. See "Filtering mail by subject line" on page 100.
Message origin	Specify one or more domains or complete email addresses that are known to be threats so that messages from these domains are rejected. See "Filtering mail by message origin" on page 102.
Attachment file name	Specify one or more file names that are known to be threats, and select whether messages that contain attachments with these file names should be rejected, or delivered with the attachment deleted. See "Filtering mail by attachment file name" on page 103.
Attachment file size	Specify file sizes of attachments, and select whether messages that contain attachments of the specified size should be rejected, or delivered with the attachment removed. See "Filtering mail by attachment file size" on page 105.
Partial messages	Reject messages that have been broken down into a number of smaller, partial messages for transmission. See "Blocking MIME partial message content" on page 106.


Limits
AntiVirus
Mail
Blocking by total message size
Block messages that are larger than 88888 bytes
Blocking by subject line
Block messages with any of the following subject lines (one per line):
LoveLetter
Gotcha
Block messages with empty subject lines
Blocking by message origin
Block messages that originate from the following email addresses or domains (one per line):
jj@jeers.com
Blocking by attachment file name
Block attachments with any of the following file names (one per line):
*.exe
When a matching attachment is found:
Delete the attachment
Reject the message
Blocking by attachment file size
Block attachments that match any of the file sizes specified below (one per line, in bytes):
456
789
444444
4323432
When a matching attachment is found:
Delete the attachment
Reject the message
Updating mail message body
Add text to body of infected MIME-encoded messages to warn recipient of infections.
Blocking MIME partial message content
Block MIME partial message content
Help
Confirm Changes

Filtering mail by total message size

You can specify a maximum size for mail messages. The maximum size includes the entire message including any attachments. Messages that exceed the maximum mail size are rejected.

A value of 0 (the default value) indicates no maximum size.

To filter mail by total message size

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the Mail tab, under Blocking by total message size, type a maximum size (in bytes) that the scan engine will accept.

   Type **0** (the default value) to indicate no maximum. Messages that are larger than the specified size are rejected.
3. When you have finished establishing the mail policy, click **Confirm Changes** to save the configuration.
4. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.

     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
   - Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

Filtering mail by subject line

To filter mail by subject, you specify one or more subject lines (or strings to be found within subject lines) that are known to be threats. Messages with these subject lines are rejected.

Subject strings that you specify are matched against the subject line of each email. Wildcard characters can be used to match when you are not sure of the exact subject line. Any white space (tabs or spaces) at the beginning of the subject line is ignored. Any white space that you enter at the beginning of your search string (the text you enter for the subject line filter) is also ignored.

Note: You can filter mail by subject line during a virus outbreak to further protect your network. In the case of a new email-borne virus, if you know the subject line or part of the subject line of the infected message, you can use this information to block infected email. You can protect your network immediately, before virus definitions for the new virus have been posted.

To filter mail by subject line

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the Mail tab, under Blocking by subject line, type a text string to block.

   Type as many subject lines to block as needed, one per line. Search strings are not case sensitive. Use the following characters as needed:

   - A question mark (?) as a wildcard to represent a single character.
   - An asterisk (*) as a wildcard to represent zero or more characters.
   - A backslash (\) as an escape character. For example, precede ? or * with \ to match a literal ? or * in a file name. To match a literal \, use \\.
3. To remove a subject from the list, select it and press **Delete**.
4. To filter mail messages that have blank subject lines, check **Block messages with empty subject lines.**
5. When you have finished establishing the mail policy, click **Confirm Changes** to save the configuration.
6. Do one of the following:

   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.

     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
   - Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

Filtering mail by message origin

To filter mail by domain, you specify one or more domain names that are known to be threats. The domain name search string that you enter is matched against addresses in the From header of the email message. If the search string matches an address, the message is rejected.

You can use this filter to block mail from specific email addresses, as well as from a specific domain. The following wildcard characters can be used to control exactly what you want to block:

- Using *@somedomain.com blocks smith@somedomain.com but does not block smith@someserver.somedomain.com.
- Using *@*somedomain.com or *somedomain.com blocks smith@somedomain.com and smith@someserver.somedomain.com.
- Using smith@somedomain.com (to block a specific email address) blocks only email from smith@somedomain.com and does not block adam_smith@somedomain.com or smith@someserver.somedomain.com.

To filter mail by message origin

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the Mail tab, under Blocking by message origin, type a domain or email address to block.

   Type as many domains or addresses to block as needed, one per line. Search strings are not case sensitive. Use the following characters as needed:

   - A question mark (?) as a wildcard to represent a single character.
   - An asterisk (*) as a wildcard to represent zero or more characters.
   - A backslash (\) as an escape character. For example, precede ? or * with \ to match a literal ? or * in a file name. To match a literal \, use \\.
3. To remove a domain name from the list, select it and press **Delete**.

4 When you have finished establishing the mail policy, click **Confirm Changes** to save the configuration.

5 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.

  If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the Scan Engine service now.
- Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

Filtering mail by attachment file name

When you filter mail by attachment file name, you specify one or more file names that are known to be threats and specify how the Symantec AntiVirus Scan Engine will handle messages that contain attachments with any of the file names listed. The scan engine can reject the entire message or deliver the message with the attachment removed. Any attachments that do not match the listed file names are not removed and are delivered with the message.

For each full file name that you want to filter, you type a separate text string. If the text string that you type matches the file name of any attachment, the message is handled accordingly.

Wildcard characters can be used when you are not sure of an exact file name or want to block all attached files with a specific extension. For example, to block all attachments with the word virus in the file name, type *virus* as the search string. To block all attachments with the .exe extension, type *.exe.

Note: You can filter mail by attachment file name during a virus outbreak to further protect your network. In the case of a new email-borne virus, if you know the file name of the infected attachment, you can use this information to block the infected email. You can protect your network immediately, before virus definitions for the new virus have been posted.

To filter mail by attachment file name

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the Mail tab, under Blocking by attachment file name, type an attachment file name to block.

   Type as many file names to block as needed, one per line. Search strings are not case sensitive. Use the following characters as needed:

   - A question mark (?) as a wildcard to represent a single character.
   - An asterisk (*) as a wildcard to represent zero or more characters.
   - A backslash (\) as an escape character. For example, precede ? or * with \ to match a literal ? or * in a file name. To match a literal \, use \\.
3. Select one of the following to specify how the scan engine will handle messages that contain an attachment with a specified file name:

   - Delete the attachment: The scan engine removes any attachments with a specified file name and delivers the remainder of the message, including attachments with file names that do not match a specified file name. The mail message is not updated to indicate that an attachment has been deleted due to a mail policy violation unless you activate the mail message update feature.

     See "Inserting text into MIME-encoded messages" on page 107.
   - Reject the message: The scan engine rejects any message that contains an attachment with a specified file name.
4. To remove a file name from the list, select it and press **Delete.**
5. When you have finished establishing the mail policy, click **Confirm Changes** to save the configuration.
6. Do one of the following:

   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.

     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
   - Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

Filtering mail by attachment file size

When you filter mail by attachment file size, you specify one or more file sizes that are known to be threats and specify how the Symantec AntiVirus Scan Engine will handle messages that contain attachments of any of the listed file sizes. The scan engine can be configured to reject the entire message or deliver the message with the attachment removed. Any attachments that do not match a specified size are not removed and are delivered with the message.

Note: You can filter mail by attachment file size during a virus outbreak to further protect your network. In the case of a new email-borne virus, if you know the exact size of the infected attachment, you can use this information to block potentially infected email messages. You can protect your network immediately, before virus definitions for the new virus have been posted.

To filter mail by attachment file size

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the Mail tab, under Blocking by attachment file size, type an attachment file size (in bytes) to block.

   Type as many file sizes to block as needed, one per line.
3. Select one of the following to specify how the scan engine will handle messages that contain attachments of a size you have specified:
   - Delete the attachment: The scan engine deletes any attachments of a specified size and delivers the remainder of the message, including attachments that do not match a specified size. The mail message is not updated to indicate that an attachment has been deleted due to a mail policy violation unless you activate the mail message update feature.

     See "Inserting text into MIME-encoded messages" on page 107.
   - Reject the message: The scan engine rejects any message that contains an attachment of a specified size.
4. To remove a file size from the list, select it and press **Delete.**

5 When you have finished establishing the mail policy, click **Confirm Changes** to save the configuration.

6 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.

  If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the Scan Engine service now.
- Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

Blocking MIME partial message content

The Symantec AntiVirus Scan Engine must have a MIME-encoded message in its entirety to effectively scan it for viruses. Some email software applications break large messages down into a number of smaller, more manageable, partial messages for transmission. These messages are typically transmitted separately and reassembled before delivery to the recipient. In these cases, because it has been broken down into a number of partial messages, the entire message (including all attachments) is not available to the scan engine for scanning. The Symantec AntiVirus Scan Engine is configured by default to reject partial messages because they cannot be effectively scanned for viruses.

To block MIME partial message content

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the Mail tab, under Blocking MIME partial message content, check **Block MIME partial message content**.

   The scan engine is configured by default to block partial messages.
3. When you have finished establishing the mail policy, click **Confirm Changes** to save the configuration.
4. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.

     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
   - Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

Inserting text into MIME-encoded messages

The Symantec AntiVirus Scan Engine can be configured to add text to the body of a MIME-encoded message to warn the recipient of the message that an attachment was infected. The mail message body also is updated when an attachment is deleted because of a mail policy violation.

The default text indicates that an attachment contained a virus and was repaired, or that it was deleted because it contained a virus that could not be repaired or that violated the mail policy. The text can be customized. The default message text is:

ALERT!!! This email contained one or more infected files. The following attachments were infected and have been repaired: <listofinfectedfiles>. The following infected attachments were deleted: <listofdeletedfiles>. The following attachments were blocked because of mail policy violations: <listofblockedfiles>. You may wish to contact the sender to inform them about their infections. Thank you, Your ISP

---------- Original message text follows ----------

Note: Even when the mail message update feature is not activated, the Symantec AntiVirus Scan Engine attaches a .txt file to mail messages in place of each attachment that is deleted because it cannot be repaired. The text file that is inserted is called deletedN.txt, where N is a sequence number. For example, if two attachments are deleted, the replacement files are called deleted1.txt and deleted2.txt. The name of the file and the text that is contained in the file can be customized by editing the message string file, symcmsgs.dat.

To insert text into MIME-encoded messages

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the Mail tab, under Updating mail message body, check **Add text to body of infected MIME-encoded messages to warn recipient of infections**.

   The default text will be used when this feature is activated unless you customize the text.
3. When you have finished establishing the mail policy, click **Confirm Changes** to save the configuration.
4. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.

     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
   - Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

Chapter 7

Configuring and using logging

This chapter includes the following topics:

- About Symantec AntiVirus Scan Engine logging
- Configuring standard logging
- Managing the standard logs
- Obtaining summary data from the standard logs
- Generating scanning statistics from the billing logs

About Symantec AntiVirus Scan Engine logging

The Symantec AntiVirus Scan Engine maintains two types of logs:

- Standard logs: Standard logs contain information on startup, shutdown, system crashes, and virus definitions updates. You can select the standard information that is logged by the Symantec AntiVirus Scan Engine. The default location for the standard logs for Solaris and Linux is /var/log/. Logging for Windows 2000 Server/Advanced Server is written to the Application Event Log.

  See "Configuring standard logging" on page 111.

- Billing logs: Billing logs contain scan volume data for the total number of files that are scanned and the average speed of processing. Scanning statistics for the billing logs are maintained automatically by the Symantec AntiVirus Scan Engine. Billing information is logged to a billing log file, symcsbps.dat.

  See "Generating scanning statistics from the billing logs" on page 121.

In addition to local logging, you can also choose to log events and alerts to the Symantec Enterprise Security Architecture (SESA). SESA includes an event management system that employs data collection services for events generated on computers that are managed by Symantec security products. SESA lets administrators view and manage the security data within a central location, the SESA Console.

See "Integrating the Symantec AntiVirus Scan Engine with SESA" on page 145.

Configuring standard logging

You can activate logging for selected scan engine activities and change the locations of key logging files. You can do any of the following:

- Change the log file location (Solaris and Linux only): To accommodate sites with specialized disk configuration, the location of the Symantec AntiVirus Scan Engine log files can be changed. The disk space that is required for the log files varies depending on scan volume and associated activity; the specified location must be large enough to accommodate these files.
  See "Changing the log file location" on page 111.
- Specify what to log: The Symantec AntiVirus Scan Engine can be configured to log a variety of events. Standard logging for the Symantec AntiVirus Scan Engine is divided into three categories of events: errors, warnings, and information. You can enable logging for an entire category or you can selectively enable logging for certain events. Logging for all errors and warnings is enabled by default.
  See "Specifying what to log" on page 112.
- Change the message string file location: The message text for Symantec AntiVirus Scan Engine alert messages, log entries, and SMTP insert messages is contained in an ASCII text file. You can change the location and file name of this file. You can customize the alert messages or log entries by editing this string file.
  See "Changing the message string file location" on page 116.
- Configure the scan engine to log events and alerts to SESA: If you are running the Symantec Enterprise Security Architecture (SESA), you can choose to log events and alerts regarding Symantec AntiVirus Scan Engine antivirus activity to SESA.
  See "Integrating the Symantec AntiVirus Scan Engine with SESA" on page 145.

Changing the log file location

If you are running the Symantec AntiVirus Scan Engine on Solaris or Linux, you can change the location of the standard and billing log files. The file names for the log files cannot be changed. The default location for the log files for Solaris and Linux is /var/log/.

If you are running the Symantec AntiVirus Scan Engine on Windows 2000 Server/Advanced Server, this setting does not appear on the administrative interface. Logging for Windows 2000 Server/Advanced Server is written to the Application Event Log.

The disk space that is required for the log files varies depending on the scan volume and associated activity; the specified location must be large enough to accommodate these files. If you change the log file location, old log files are left in the old directory and are not removed on uninstall. Old logs must be removed manually.

To change the log file location

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Logging tab, under Log file location, type the path to the new location for the log file.

   The default location for the log files for Solaris and Linux is /var/log/.
3. Click **Confirm Changes** to save the configuration.

   You must restart the Symantec AntiVirus Scan Engine service for this change to take effect. Data that was logged prior to restarting the service is contained in the previous log file and is not parsed for Symantec AntiVirus Scan Engine reporting purposes.
4. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.

     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
   - Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

Specifying what to log

Standard logging for the Symantec AntiVirus Scan Engine is divided into three categories of events to be logged: errors, warnings, and information. You can enable logging for an entire category, or you can selectively enable logging for certain events.

If you activate logging by category, you do not need to enable the individual events in that category. Table 7-1 shows the specific events that are included in each category.

Table 7-1 Logging events by category

Log All option	Events included in the Log All option
Log all errors	■ Server crash ■ Virus definition update error ■ Threshold number of queued requests exceeded ■ Error sending SNMP/SMTP alert ■ License expired
Log all warnings	■ Infection found ■ Non-repairable infection found ■ License about to expire
Log all information	■ Server start ■ Server stop ■ Virus definition update

You can enable logging for selected events. Table 7-2 defines each individual logging option.

Table 7-2 Individual logging options

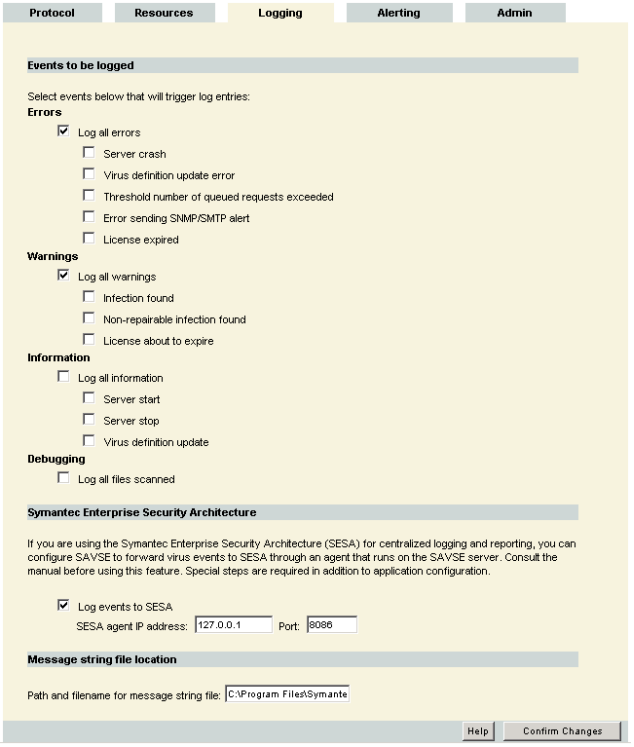
Logging option	Description
Server crash	Logs all instances of scan engine crashes
Virus definition update error	Logs all errors that occur in virus definitions updates
Threshold number of queued requests exceeded	Logs all instances when the threshold number of queued requests is exceeded for the scan engine (log entries are generated based on the selected alert interval)
Error sending SNMP/SMTP alert	Logs all errors in sending alerts that result in no alert being sent (neither the primary nor the secondary SMTP server was available) **Note:** Because the broadcast nature of SNMP prevents the detection of transmission failure, no log entry is generated when an SNMP alert is not received because the SNMP console is down or the IP address for the SNMP console is entered incorrectly.

Table 7-2 Individual logging options

Logging option	Description
License expired	Logs each 24-hour period following a Symantec AntiVirus Scan Engine license expiration **Note:** Log entries for an expired license are generated only during the grace period following the license expiration date. If the grace period expires before the license is renewed, all record of the existing license is removed and the product or feature becomes unlicensed.
Infection found	Logs all infections found in scanned files
Non-repairable infection found	Logs all infections found that cannot be repaired **Note:** When the Symantec AntiVirus Scan Engine is set to Scan Only, this log entry is generated for any infection found.
License about to expire	Logs each 24-hour period when a Symantec AntiVirus Scan Engine license is about to expire (that is, the license is within 30 days of its expiration date)
Server start	Logs all instances of scan engine startup
Server stop	Logs all instances of scan engine shutdown
Virus definition update	Logs all instances of scan engine virus definitions updates
Debugging only: Log all files scanned	Logs all files scanned **Note:** This logging option is Off by default even when all three Log All options are enabled. This option should be enabled only for debugging purposes. Activating this logging option for general logging degrades performance significantly.

To specify what to log for the Symantec AntiVirus Scan Engine

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Logging tab, under Events to be logged, under Errors, do one of the following:
   - Check **Log all errors** to enable logging for all errors.
   - Check individual options for any specific events to be logged.


Protocol
Resources
Logging
Alerting
Admin
Events to be logged
Select events below that will trigger log entries:
Errors
Log all errors
Server crash
Virus definition update error
Threshold number of queued requests exceeded
Error sending SNMP/SMTP alert
License expired
Warnings
Log all warnings
Infection found
Non-repairable infection found
License about to expire
Information
Log all information
Server start
Server stop
Virus definition update
Debugging
Log all files scanned
Symantec Enterprise Security Architecture
If you are using the Symantec Enterprise Security Architecture (SESA) for centralized logging and reporting, you can configure SAVSE to forward virus events to SESA through an agent that runs on the SAVSE server. Consult the manual before using this feature. Special steps are required in addition to application configuration.
Log events to SESA
SESA agent IP address: 127.0.0.1
Port: 8086
Message string file location
Path and filename for message string file: C:\Program Files\Symante
Help
Confirm Changes

3. Under Warnings, do one of the following:
   - Check **Log all warnings** to enable logging for all warnings.
   - Check individual options for any specific events to be logged.
4. Under Information, do one of the following:
   - Check **Log all information** to enable logging for all activity.
   - Check individual options for any specific events to be logged.

5. If you have been instructed to do so for debugging purposes by Symantec Technical Service and Support, under Debugging, check **Log all files scanned** to generate a log entry for every file that is scanned.
6. Click **Confirm Changes** to save the configuration.
7. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.

     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
   - Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

Changing the message string file location

The message text for Symantec AntiVirus Scan Engine alert messages, log entries, and SMTP insert messages is contained in an ASCII text file. You can change the location and file name of this file.

Symantec AntiVirus Scan Engine alert messages can be customized by editing the string file.

To change the message string file location

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Logging tab, under Message string file location, type a path and file name to change the message string file location and file name.

   The default location for Solaris and Linux is /opt/SYMCScan/etc/symcsmsg.dat. The default location for Windows 2000 Server/Advanced Server is C:\Program Files\Symantec\Scan Engine\symcsmg.dat.
3. Click **Confirm Changes** to save the configuration.
4. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.

     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
   - Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

Managing the standard logs

You can download the standard log file in a selected format to a remote computer and save the data to a file, or you can clear the standard log file.

You can download the log file in a comma-separated value (CSV) format for export to a file or in an HTML table format that displays in the browser window. This lets you save or review log data in a usable format. The amount of data that can be downloaded is limited so as not to overwhelm the browser or the server. You can download one or two megabytes of data. The data that is returned is the most recent log entries.

Note: If you attempt to download large log files during periods of peak usage, Symantec AntiVirus Scan Engine performance may be impacted.

You also can clear the Symantec AntiVirus Scan Engine log file. This lets you keep the log file at a manageable size. Clearing the log file erases all of the log entries in the file. To retain access to the log data, download the log and export the data to another file prior to clearing the log file. Logging continues from the date and time that you clear the logs.

Warning: For Windows 2000 Server/Advanced Server, clearing the log file causes all of the application logs to be cleared, not just those for the Symantec AntiVirus Scan Engine.

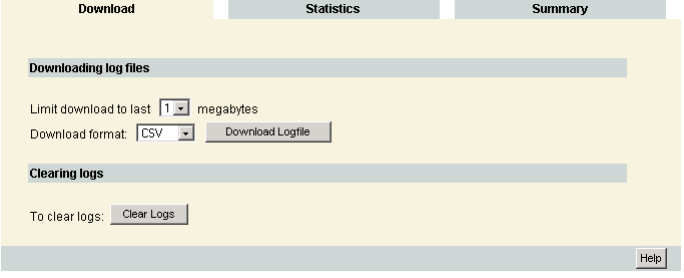
To manage log files

You can download or clear the log file.

To download the log file

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Reporting**.
2. On the Download tab, under Downloading log files, select the amount of data, in megabytes, to download.

   The size of the download is limited to one or two MB so that the amount of data that is returned does not overwhelm the browser or your server.



3 In the Download format drop-down list, select one of the following:

- CSV: You can open the text file directly or save the file to a specified location.
- HTML table: The data displays in the browser window in an HTML table format.

4 Click **Download Logfile**.

Sample HTML table output

DATE	TYPE	ACTION
[Mon Mar 25 16:39:30 2002]	I	The Scan Engine has just started up.
[Mon Mar 25 14:41:28 2002]	I	The Scan Engine has been manually shut down.
[Mon Mar 25 14:41:17 2002]	I	The Scan Engine has just started up.
[Mon Mar 25 14:38:05 2002]	I	The Scan Engine has been manually shut down.
[Mon Mar 25 14:37:42 2002]	I	The Scan Engine has just started up.
[Mon Mar 25 14:31:07 2002]	I	The Scan Engine has been manually shut down.
[Mon Mar 25 14:30:46 2002]	I	The Scan Engine has just started up.
[Mon Mar 25 14:29:06 2002]	I	The Scan Engine has been manually shut down.
[Mon Mar 25 14:28:54 2002]	I	The Scan Engine has just started up.
[Mon Mar 25 14:27:34 2002]	I	Symantec AntiVirus Scan Engine Logging Stopped

To clear the log file

1 On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Reporting**.

2 On the Download tab, click **Clear Logs**.

3 Confirm that you want to clear the application log.

Warning: For Windows 2000 Server/Advanced Server, clearing the log file causes all of the application logs to be cleared, not just those for the Symantec AntiVirus Scan Engine.

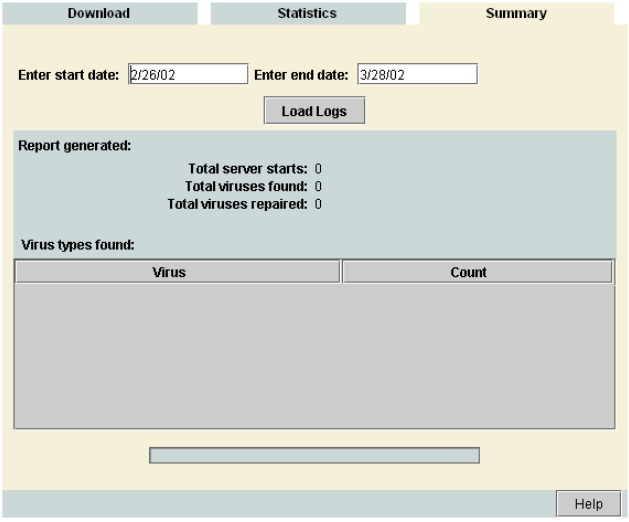
Obtaining summary data from the standard logs

You can obtain summary data from the standard logs for a given period of time. For the reported period, you can review the number of times that the scan engine started, the total number of viruses that were found, and the total number of viruses that were repaired. You can also review the virus types that were found during the reported period and the number of times that each type was found.

To obtain summary data from the standard logs

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Reporting**.
2. On the Summary tab, type start and end dates for the range on which you want to report.

   Use the date format for your operating system locale.

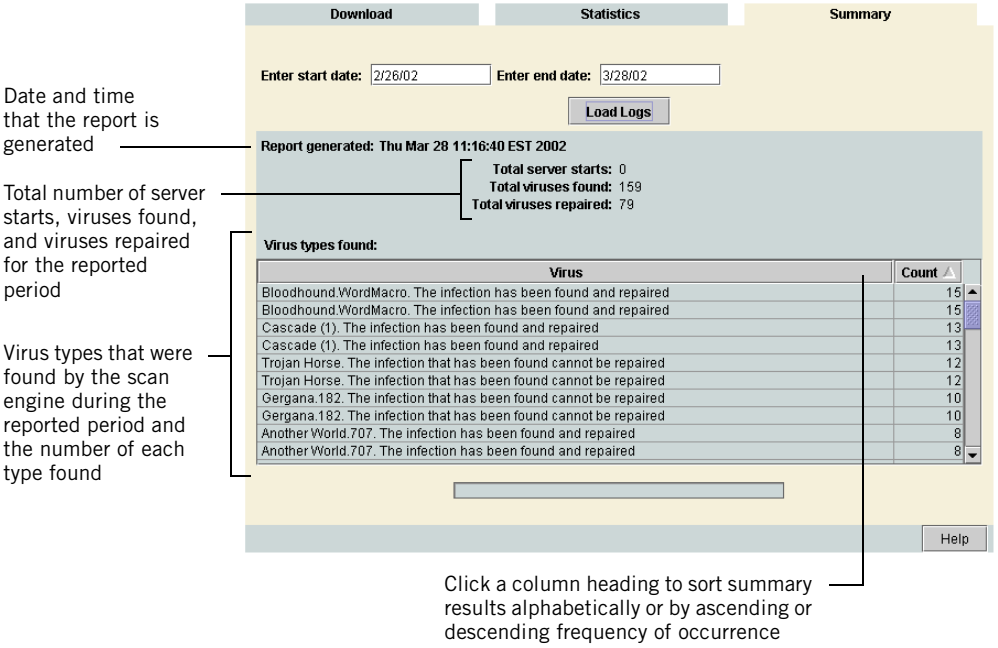


3. Click **Load Logs**.

   The log data for the requested period displays in the browser window.

Interpreting summary data from the standard logs

Sample summary data from the standard logs is shown in the figure below.


Download
Statistics
Summary
Enter start date: 2/26/02
Enter end date: 3/28/02
Load Logs
Report generated: Thu Mar 28 11:16:40 EST 2002
Total server starts: 0
Total viruses found: 159
Total viruses repaired: 79
Virus types found:
Virus
Count
Bloodhound.WordMacro. The infection has been found and repaired 15
Bloodhound.WordMacro. The infection has been found and repaired 15
Cascade (1). The infection has been found and repaired 13
Cascade (1). The infection has been found and repaired 13
Trojan Horse. The infection that has been found cannot be repaired 12
Trojan Horse. The infection that has been found cannot be repaired 12
Gergana.182. The infection that has been found cannot be repaired 10
Gergana.182. The infection that has been found cannot be repaired 10
Another World.707. The infection has been found and repaired 8
Another World.707. The infection has been found and repaired 8
Help
Date and time that the report is generated
Total number of server starts, viruses found, and viruses repaired for the reported period
Virus types that were found by the scan engine during the reported period and the number of each type found
Click a column heading to sort summary results alphabetically or by ascending or descending frequency of occurrence

Generating scanning statistics from the billing logs

The Symantec AntiVirus Scan Engine maintains scanning statistics to support billing for antivirus scanning that is based on megabits-per-second-per-month and file-based billing schemes. Each time that a file is scanned, the Symantec AntiVirus Scan Engine submits scan statistics to an encrypted data file. You can examine these scanning statistics.

If you bill customers based on bandwidth consumption, you can use this bandwidth metering component to measure the number of megabits-per-second-per-month that are scanned by each Symantec AntiVirus Scan Engine. The scan engine implements the 95th percentile bandwidth measurement scheme, making it easy for you to add an additional charge for antivirus scanning to existing megabits-per-second-per-month-based billing statements.

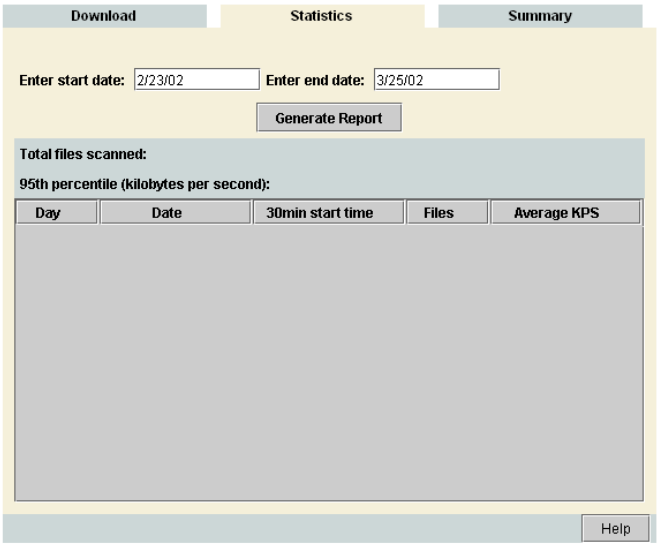
See "Understanding the 95th percentile bandwidth measurement" on page 124.

The Symantec AntiVirus Scan Engine also tracks each file that is scanned for file-based billing schemes.

Billing information is logged to a billing log file, symcsbps.dat. The default location for the file for Solaris and Linux is /var/log/symcsbps.dat. The default location for Windows 2000 Server/Advanced Server is C:\Program Files\Symantec\Scan Engine\symcsbps.dat. If you specified a different directory for the log files, the billing log file is located in that directory. The Symantec AntiVirus Scan Engine maintains scanning statistics for the previous eight months.

To generate scanning statistics from the billing logs

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Reporting**.
2. On the Statistics tab, type start and end dates for the range on which you want to report.



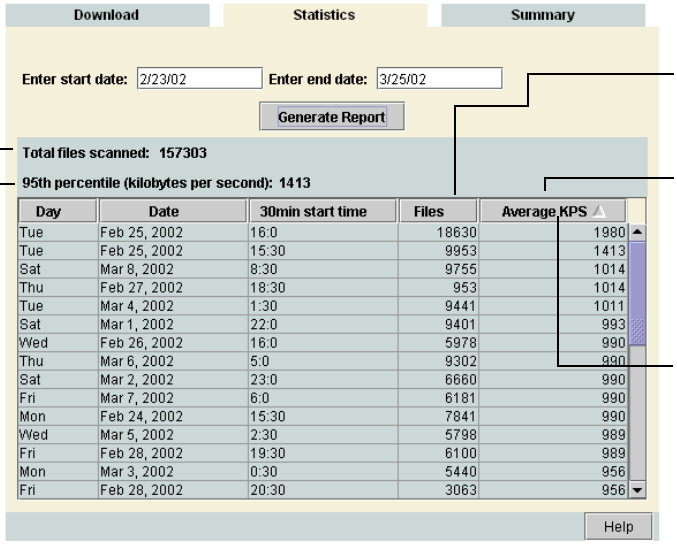
3. Click **Generate Report**.
   The data for the requested period displays in the browser window.

Interpreting scanning statistics

The scanning statistics that are maintained by the Symantec AntiVirus Scan Engine support billing for antivirus scanning based on megabits-per-second-per-month and file-based billing schemes. You can examine these scanning statistics for a given time range in one of two ways. You can retrieve data via the Statistics tab on the Symantec AntiVirus Scan Engine administrative interface (recommended), or you can use the getstat utility, which also is included with the Symantec AntiVirus Scan Engine, to obtain statistical data via the command line.

See "Generating scanning statistics from the billing logs" on page 121.

A sample report that was generated through the administrative interface is shown in the figure below.


Download
Statistics
Summary
Enter start date: 2/23/02
Enter end date: 3/25/02
Generate Report
Total files scanned: 157303
95th percentile (kilobytes per second): 1413
Day | Date | 30min start time | Files | Average KPS
Tue | Feb 25, 2002 | 16:0 | 18630 | 1980
Tue | Feb 25, 2002 | 15:30 | 9953 | 1413
Sat | Mar 8, 2002 | 8:30 | 9755 | 1014
Thu | Feb 27, 2002 | 18:30 | 953 | 1014
Tue | Mar 4, 2002 | 1:30 | 9441 | 1011
Sat | Mar 1, 2002 | 22:0 | 9401 | 993
Wed | Feb 26, 2002 | 16:0 | 5978 | 990
Thu | Mar 6, 2002 | 5:0 | 9302 | 990
Sat | Mar 2, 2002 | 23:0 | 6660 | 990
Fri | Mar 7, 2002 | 6:0 | 6181 | 990
Mon | Feb 24, 2002 | 15:30 | 7841 | 990
Wed | Mar 5, 2002 | 2:30 | 5798 | 989
Fri | Feb 28, 2002 | 19:30 | 6100 | 989
Mon | Mar 3, 2002 | 0:30 | 5440 | 956
Fri | Feb 28, 2002 | 20:30 | 3063 | 956
Help
Total number of files that were scanned for the reported period
95th percentile bandwidth measurement for the reported period
Number of files that were scanned for each 30-minute period
Calculated average KPS for each 30-minute period (identified by start time)
Clicking a column heading sorts the entries by that criteria

The total number of files that were scanned should not be interpreted strictly as a physical file count. This total includes the number of files as well as additional objects within container files that were scanned. Some containers, such as MIME-encoded messages and Microsoft Office documents, have additional embedded objects that are not files but that may be scanned depending on the files that you have selected for scanning (the extension list settings). The total does not include any objects within container files that were not scanned because the object's extension did not match those that were selected for scanning.

For each 30-minute period that is in the specified date range, the total number of files that were scanned and the average KPS scanned for that 30-minute increment are reported. The 30-minute time periods are reported in Greenwich mean time (GMT).

Note: The getstat utility reports the 95th percentile bandwidth measurement as a bits-per-second (bps) measurement rather than a kilobytes-per-second (KPS) measurement as through the interface. For information on how the 95th percentile measurement is calculated, see "Understanding the 95th percentile bandwidth measurement" on page 124.

Understanding the 95th percentile bandwidth measurement

The 95th percentile bandwidth measurement is based on a bits-per-second (bps) measurement. The Symantec AntiVirus Scan Engine tallies the number of bits for each file that is scanned in 30-minute increments. The average bps scanned for each 30-minute period is calculated and saved to the billing file. (Data is saved to the billing file every five minutes to prevent the loss of data in the event that the scan engine crashes.) The Symantec AntiVirus Scan Engine logs the average bps that are scanned for 48 30-minute periods per day.

To make a data retrieval request, you specify a date range for which to view scan engine utilization. When a request is made, the data entries for each 30-minute period in the specified date range are sorted from highest to lowest average bps scanned. Of these entries, the top five percent (with the highest average bandwidth scanned) represent spikes in usage and are discarded. The next highest reading is considered the 95th percentile bandwidth measurement.

Note: The 95th percentile bandwidth measurement scheme is designed for billing for maximum bandwidth utilization and assumes that a system is used continuously rather than being shut down and restarted routinely.

Chapter 8

Configuring LiveUpdate

This chapter includes the following topics:

- About LiveUpdate
- Updating virus definitions
- Scheduling LiveUpdate via the command line
- Setting up your own LiveUpdate server

About LiveUpdate

LiveUpdate ensures that your network is not at risk of infection by newly discovered viruses. For Solaris and Linux, the Symantec AntiVirus Scan Engine features Symantec Java LiveUpdate technology, which is found in other Symantec antivirus products for these platforms. For Windows 2000 Server/Advanced Server, a LiveUpdate client is installed with the Symantec AntiVirus Scan Engine. On all platforms, the Symantec AntiVirus Scan Engine can be updated with the latest virus definitions without any interruption of virus scanning.

Note: To run LiveUpdate on Solaris or Linux, you must have Java version 1.2 or later.

Updated virus definitions files, which contain the necessary information to detect and eliminate viruses, are supplied by Symantec at least every week and whenever a new virus threat is discovered. When new virus definitions files are available, the LiveUpdate technology automatically downloads the proper files and installs them in the proper location. If an error occurs, the Symantec AntiVirus Scan Engine attempts to roll back to the previous virus definitions and continue scanning. If the rollback is unsuccessful, scanning is disabled.

You can update virus definitions files and schedule LiveUpdate to run automatically so that you always have the most up-to-date protection.

See "Updating virus definitions" on page 126.

You can also schedule LiveUpdate via the command line, if necessary.

See "Scheduling LiveUpdate via the command line" on page 128.

Updating virus definitions

You can schedule LiveUpdate to run automatically, and you can force LiveUpdate to run immediately to obtain updated virus definitions when necessary. Scheduling LiveUpdate to occur automatically at a specified time interval ensures that the Symantec AntiVirus Scan Engine always has the most current virus definitions. You should schedule LiveUpdate so that you do not have to remember to update virus definitions regularly.

When necessary, you can run LiveUpdate manually. This forces an immediate LiveUpdate attempt. If you have scheduled LiveUpdate, the next scheduled LiveUpdate attempt occurs as directed.

You can also get the date and revision number of the virus definitions updates that the Symantec AntiVirus Scan Engine is currently using. These display automatically on the LiveUpdate tab. You may need to know the current version that the scan engine is using for Symantec Service and Support. You can also determine the status of the last LiveUpdate attempt.

To update virus definitions

You can manually run LiveUpdate or you can schedule LiveUpdate to occur automatically.

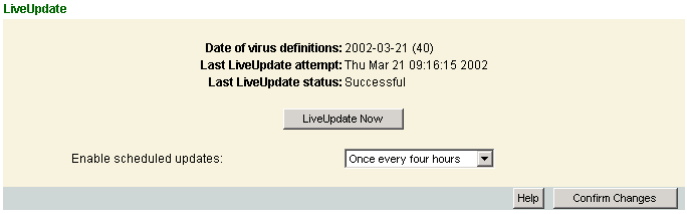
Note: When you schedule LiveUpdate for the Symantec AntiVirus Scan Engine for the first time, a LiveUpdate attempt occurs immediately following the required restart of the Scan Engine service. The timestamp for this initial LiveUpdate is used to set the selected interval for subsequent LiveUpdate attempts. Subsequent restarts of the scan engine will not trigger a LiveUpdate attempt. If you change the scheduled LiveUpdate interval, the interval adjusts based on the timestamp of the last LiveUpdate attempt.

To update virus definitions manually

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **LiveUpdate**.
2. Click **LiveUpdate Now**.
   The screen refreshes to indicate whether the LiveUpdate was successful.

To schedule LiveUpdate to update virus definitions automatically

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **LiveUpdate**.



2. In the Enable scheduled updates drop-down list, select the desired interval.
   This setting is Off by default.
3. Click **Confirm Changes** to save the configuration.

Scheduling LiveUpdate via the command line

You can also schedule LiveUpdate via the command line to ensure that the Symantec AntiVirus Scan Engine always has the most current virus definitions. On Solaris and Linux, virus definitions updates can be scheduled using the UNIX cron scheduler and a shell script.

The cslive.exe client can be run from the command line to update virus definitions for the Symantec AntiVirus Scan Engine for Windows 2000 Server/ Advanced Server.

To schedule LiveUpdate via the command line

You can schedule LiveUpdate on UNIX and Windows platforms via the command line.

To schedule LiveUpdate via the UNIX cron scheduler (Solaris and Linux)

1. Create a user called symantec.
2. Open the /etc/group file and type **symantec** at the end of the avdefs line.
   For more information, see the group man pages.
3. Change directories to /etc/cron.d.
4. Create a file called cron.allow.
   This file contains the list of users that are allowed to use cron services.
5. Add the following line to the file:
   symantec
   For more information, see the cron and crontab man pages.
6. Run crontab -e symantec, and add the following line:
   0 * * * * /usr/bin/sh /opt/SYMCScan/bin/liveupdate.sh -virusdefs -silent > /dev/null
   The cron scheduler will run the LiveUpdate script once per hour. For more information, see the cron and crontab man pages.

To run LiveUpdate on Windows 2000 Server/Advanced Server

- At the command prompt, type one of the following commands:
  - cslive.exe /virusdefs /silent: Run LiveUpdate in silent mode (no prompting or display indicator).
  - cslive.exe /virusdefs: Run LiveUpdate and display a progress indicator.

LiveUpdate should be scheduled to run periodically (at least weekly) by using the Windows at command. For example:

at 02:00 every:M C:\Program Files\Symantec\Scan Engine\cslive.exe /virusdefs /silent

This command runs LiveUpdate every Monday at 2:00 AM with no user intervention (/silent).

Setting up your own LiveUpdate server

Depending on your network setup and the number of Symantec AntiVirus Scan Engines that you have installed on your network, you may want to set up your own LiveUpdate server rather than have each scan engine on your network contact Symantec servers.

For more information, see the *LiveUpdate Administration Utility*, which is included on the Symantec AntiVirus Scan Engine CD.

If you set up your own LiveUpdate server, you will need to edit the LiveUpdate configuration for the Symantec AntiVirus Scan Engine to point to the local LiveUpdate server. For Solaris and Linux, the Symantec AntiVirus Scan Engine LiveUpdate configuration file contains the configuration options for LiveUpdate (the default location is /etc/liveupdate.conf). For Windows 2000 Server/ Advanced Server, a LiveUpdate client, cslive.exe, is installed with the Symantec AntiVirus Scan Engine. Contact Symantec Service and Support for more information.

Chapter 9

Customizing log entries and alert messages

This chapter includes the following topics:

- About the message string file
- Editing the message string file
- About alert strings
- About alert text for MIME-encoded messages
- About log entries
- Editing the ICAP access denied message

About the message string file

Symantec AntiVirus Scan Engine alert messages can be customized by editing the message string file.

The message string numbers in the file identify the usage for the message string. The message strings are numbered as follows:

- 1000 series: Message strings that are numbered in this manner are used to build the SNMP and SMTP alerts and standard log entries. Log entries and SMTP and SNMP alerts can be generated for many activities, including start-up, shutdown, virus definitions updates, infections found, and so on.
  See Table 9-1, “Alert string usage,” on page 133.
- 2000 series: Message strings that are numbered in this manner are used to update email messages when an infected attachment is found and repaired or deleted (because it cannot be repaired). This type of alert message notifies the recipient of a scanned email message that one or more attachments that were contained in the message were infected. Variables can be used to customize these alert messages.
  See Table 9-2, “Default alert text for MIME-encoded messages,” on page 138.
- 4000 series: Message strings that are numbered in this manner are used to build log entries.
  See Table 9-4, “Default log text and usage,” on page 141.

Editing the message string file

Unless you have changed the location and file name of this file, the default location for Solaris and Linux is /opt/SYMCScan/etc/symcsmsg.dat. For Windows 2000 Server/Advanced Server, the default location is C:\Program Files\Symantec\Scan Engine\symcsmg.dat.

To edit the Symantec AntiVirus Scan Engine message string file

1. Locate the Symantec AntiVirus Scan Engine message string file and open it with a text editor.
2. Make your changes to the file.
3. Save the changes to the file.
4. Stop and restart the Symantec AntiVirus Scan Engine.

About alert strings

In most cases you will not need to edit alert strings, but you can customize alert messages for the Symantec AntiVirus Scan Engine if necessary.

Double-byte characters are supported for the scan engine alert string text. For each message string file entry, the text that follows the space after the string number and before the *** can be edited.

Each string file entry that is used in generating Symantec AntiVirus Scan Engine alerts is described in Table 9-1.

Table 9-1 Alert string usage

No.	Default alert text	Description
1001	Scan Engine IP address:<IPaddress>	The IP address of the Symantec AntiVirus Scan Engine that is the subject of the alert
1002	Scan Engine port number:<portnumber>	The port number of the Symantec AntiVirus Scan Engine that is the subject of the alert
1003	Scan Engine virus fingerprint date:<virus fingerprintdate>	The date on which the virus definitions that are the subject of the alert were created (for virus update or update error)
1004	Scan Engine threshold queue size:<queuesize>	The threshold queue size for the Symantec AntiVirus Scan Engine that is the subject of the alert
1005	Scan Engine number of queued items:<queueditems>	The number of queued scan requests for the Symantec AntiVirus Scan Engine at the time of the reported event
1006	Date/time of event:<date/time>	The date and time of the reported event (Symantec AntiVirus Scan Engine crash, startup, shutdown, and so on)
1007	System uptime (in seconds):<time>	The amount of time (at the time of the alert) that the Symantec AntiVirus Scan Engine has been running since the last crash or since startup
1008	Scan Engine Crash Alert	Subject of the Symantec AntiVirus Scan Engine Crash Alert
1009	The Scan Engine has crashed.	Message body text for the Symantec AntiVirus Scan Engine Crash Alert

Table 9-1 Alert string usage

No.	Default alert text	Description
1010	Scan Engine Startup Alert	Subject of the Symantec AntiVirus Scan Engine Startup Alert
1011	The Scan Engine has just started up.	Message body text for the Symantec AntiVirus Scan Engine Startup Alert
1012	Scan Engine Shutdown Alert	Subject of the Symantec AntiVirus Scan Engine Shutdown Alert
1013	The Scan Engine has been manually shut down.	Message body text for the Symantec AntiVirus Scan Engine Shutdown Alert
1014	Scan Engine Virus Definition Update Alert	Subject of the Symantec AntiVirus Scan Engine Virus Definition Update Alert
1015	The Scan Engine has updated its virus definitions.	Message body text for the Symantec AntiVirus Scan Engine Virus Definition Update Alert
1016	Scan Engine Queue Overflow	Subject of the Symantec AntiVirus Scan Engine Load Exceeded Alert
1017	The Scan Engine queue is backing up due to a large number of requests.	Message body text for the Symantec AntiVirus Scan Engine Load Exceeded Alert
1018	Scan Engine Virus Definition Update Error Alert	Subject of the Symantec AntiVirus Scan Engine Virus Definition Update Error Alert, which is issued when an error occurs in updating the virus definitions and scanning is disabled
1019	There was an error loading/ finding the Scan Engine virus definitions. All scanning will be disabled.	Message body text for the Symantec AntiVirus Scan Engine Virus Definition Update Error Alert, which is issued when an error occurs in updating the virus definitions and scanning is disabled
1020	Scan Engine Virus Definitions Update Failure Alert	Subject of the Symantec AntiVirus Scan Engine Virus Definitions Update Failure Alert, which is issued when an error occurs in updating the virus definitions, but scanning continues using the previous virus definitions

Table 9-1 Alert string usage

No.	Default alert text	Description
1021	There was an error loading/ finding new Scan Engine virus definitions. Scanning will continue using the original definitions.	Message body text for the Symantec AntiVirus Scan Engine Virus Definitions Update Failure Alert, which is issued when an error occurs in updating the virus definitions, but scanning continues using the previous virus definitions
1022	Scan Engine Virus Definitions Update and Rollback Failure Alert	Subject of the Symantec AntiVirus Scan Engine Virus Definitions Update and Rollback Failure Alert, which is issued when an error occurs in updating the virus definitions and rollback to previous virus definitions is unsuccessful
1023	There was an error loading/ finding new Scan Engine virus definitions. An attempt to roll back to the previous definitions has also failed. All scanning will be disabled.	Message body text for the Symantec AntiVirus Scan Engine Virus Definitions Update and Rollback Failure Alert, which is issued when an error occurs in updating the virus definitions and rollback to previous virus definitions is unsuccessful
1024	Scan Engine Infection Found Alert	Subject of the Symantec AntiVirus Scan Engine Infection Found Alert
1025	The Scan Engine has resumed scanning using its previous virus definitions.	Message text for the log entry that is issued when an error has occurred in updating the virus definitions and rollback to previous virus definitions is successful
1026	Scan Engine Nonrepairable Infection Found Alert	Subject of the Symantec AntiVirus Scan Engine Nonrepairable Infection Found Alert
1027	The infection that has been found cannot be repaired.	Message body text for the Symantec AntiVirus Scan Engine Nonrepairable Infection Found Alert
1028	Virus name:	Message body text that states the virus name for both the Infection Found Alert and Nonrepairable Infection Found Alert The Symantec AntiVirus Scan Engine automatically inserts the virus name.

Table 9-1 Alert string usage

No.	Default alert text	Description
1029	Virus ID:	Message body text that states the virus ID number for both the Infection Found Alert and Nonrepairable Infection Found Alert The Symantec AntiVirus Scan Engine automatically inserts the virus ID.
1030	Disposition:	Message body text that states the disposal method of the infected file for both the Infection Found Alert and Nonrepairable Infection Found Alert The Symantec AntiVirus Scan Engine automatically inserts the disposal method for the file.
1031	An infection has been found but no repair has been attempted.	Message body text for the Infection Found Alert when the Symantec AntiVirus Scan Engine is configured to scan files but not to attempt repairs
1032	The infection has been found and repaired.	Message body text for the Infection Found Alert when the infected file can be repaired and the Symantec AntiVirus Scan Engine is configured to repair infected files
1035	Scan Engine Mail Policy Initialization Error	Subject of the Symantec AntiVirus Scan Engine Mail Policy Initialization Error log entry Logging for this event is activated when you select Server crash as an event to log or when you have Log all errors selected.
1036	There was an error loading/ finding the Scan Engine mail policy configuration files. Please correct the problem and restart the Scan Engine.	Message text for the Symantec AntiVirus Scan Engine Mail Policy Initialization Error log entry that is issued when a mail policy configuration file is missing
1037	Symantec AntiVirus Scan Engine Logging Stopped	Message text for the log entry that is issued when logging stops for the Symantec AntiVirus Scan Engine (because the scan engine has been shut down or has crashed)

Table 9-1 Alert string usage

No.	Default alert text	Description
1038	A license is about to expire:	Message body text for the Scan Engine Licensing Alert when a Symantec AntiVirus Scan Engine license is about to expire (that is, the license is within 30 days of its expiration date)
1039	A license has expired:	Message body text for the Scan Engine Licensing Alert when a Symantec AntiVirus Scan Engine license has expired This alert is generated only while the scan engine is operating in the grace period.
1040	Scan Engine Licensing Alert	Subject of the Scan Engine Licensing Alert
1041	Feature Name:	Message body text that states the feature name for the license that is the subject of the Scan Engine Licensing Alert
1042	Expiration Date:	Message body text that states the expiration date for the license that is the subject of the Scan Engine Licensing Alert
1043	Consult the license Status page for more information.	Additional message body text for the Scan Engine Licensing Alert when a Symantec AntiVirus Scan Engine license has expired or is about to expire
1101	CLEAN	Message body text that appears to the right of Disposition to indicate that no virus has been found
1102	NOT REPAIRED	Message body text that appears to the right of Disposition to indicate that a virus has been found, but the infected file has not been repaired
1103	PARTIALLY REPAIRED	Message body text that appears to the right of Disposition to indicate that multiple viruses have been found, but not all of the viruses could be eliminated from the infected file
1104	REPAIRED	Message body text that appears to the right of Disposition to indicate that a virus has been found and the file has been repaired

Table 9-1 Alert string usage

No.	Default alert text	Description
1110	DELETED	Message body text that appears to the right of Disposition to indicate that a virus has been found, but the file could not be repaired and has been deleted

About alert text for MIME-encoded messages

The 2000-series strings are used to update email messages when an infected attachment is found and repaired or deleted (because it cannot be repaired). These alert messages are intended to notify the recipient of a scanned email message that one or more attachments that were contained in the message were infected.

Note: In order for this type of alert message to be added to MIME-encoded messages, the Symantec AntiVirus Scan Engine must be configured to update messages in this manner.

See "Inserting text into MIME-encoded messages" on page 107.

The message strings that are used to update MIME-encoded messages are described in Table 9-2.

Table 9-2 Default alert text for MIME-encoded messages

No.	Default alert text	Description
2000	ALERT!!! This email contained one or more infected files. The following attachments were infected and have been repaired: <listofinfectedfiles>. The following infected attachments were deleted: <listofdeletedfiles>. The following attachments were blocked because of mail policy violations: <listofblockedfiles>. You may wish to contact the sender to inform them about their infections. Thank you, Your ISP ---------- Original message text follows ----------	This alert message text is inserted into the body of MIME-encoded, text-only messages when an infected attachment is found and repaired, or deleted from the message. Alert message strings 2000 and 2001 should be identical so that the inserted message is consistent. **Note:** <listofinfectedfiles> is generated by the variable **R, <listofdeletedfiles> is generated by the variable **D, and <listofblockedfiles> is generated by the variable **P. See Table 9-3, "Variables for customizing message strings," on page 141.

Table 9-2 Default alert text for MIME-encoded messages

No.	Default alert text	Description
2001	Repeat of message string 2000	Message text that is inserted into the body of MIME-encoded messages that contain HTML when an infected attachment is found and repaired or deleted from the message. Default message text is the same for message strings 2000 and 2001. These two messages should be consistent.
2002	No attachments are in this category.	Text that is inserted into message string 2000 or 2001 when no attachments are applicable for the variables **D, **R, or **P.
2003	Mail Policy Block (Attachment Name)	Text that replaces the <virusname> variable in message string 4000 when an attachment is deleted because it violates the mail policy that was established for attachment file name.
2004	Mail Policy Block (Attachment Size)	Text that replaces the <virusname> variable in message string 4000 when an attachment is deleted because it violates the mail policy that was established for attachment file size.
2005	Mail Policy Block	Text that replaces the <virusname> variable in message string 4000 when an email message is blocked because it violates the established mail policy.

Table 9-2 Default alert text for MIME-encoded messages

No.	Default alert text	Description
2010	DELETED**C.TXT	File name for the file that is substituted in a MIME-encoded message for any attachment that is deleted because it contains an unrepairable virus. When a message contains more than one infected file, a separate deleted.txt file is created for each file. The files are numbered sequentially beginning with 0 using the **C variable in the file name. **Note:** If you are using the native protocol, AVSCANREPAIRDELETE must be used for deleted.txt to replace deleted files. If you are using ICAP, the scan policy must be set to Scan and repair or delete. (The Symantec AntiVirus Scan Engine must be configured to delete any infected attachments from MIME-encoded messages.)
2011	file attachment: The file attached to this email was removed because it is infected with the <virusname> virus.	Text that is contained in the deleted.txt file, which is substituted in a MIME-encoded message for any attachment that is deleted because it contains an unrepairable virus.

Several variables can be used to customize the 2000 and 2001 message strings. These variables are described in Table 9-3.

Table 9-3 Variables for customizing message strings

Variable	Description
**N	Moves to the next line (text only)
 	Moves to the next line (HTML only)
**R	Displays a list of all of the infected attachments that have been repaired for a message
**D	Displays a list of all of the infected attachments that have been deleted for a message because they could not be repaired
**I	Displays a list of all of the infected attachments that were identified for a message, whether they were deleted or repaired
**P	Displays a list of all of the attachments that were deleted for a message because of mail policy violations

About log entries

The 4000-series message strings are used in log entries (when logging is enabled). These message strings are described in Table 9-4.

Table 9-4 Default log text and usage

No.	Default log text	Description
4000	A virus or other malicious code has been detected.<filename:virus name>	A virus was detected, or an attachment or mail message was blocked due to a mail policy violation (appropriate logging must be enabled)
4001	A file has been received and scanned.<filename>	A file was scanned (Log all files scanned must be activated to induce logging of every file that is scanned)
4002	Error trying to send an SMTP/SNMP alert.	SMTP or SNMP alerting failed, for example, if the SMTP server was unreachable
4010	was	Used in message string 4012 to indicate that a file was infected (but is no longer infected because it has been repaired)

Table 9-4 Default log text and usage

No.	Default log text	Description
4011	is	Used in message string 4012 to indicate that a file was infected (and is still infected because no repair has been attempted, or it cannot be repaired)
4012	File %s %s infected with virus %s.	Used when an infection is found to indicate the name of the infected file, whether the file was or is still infected, and the virus name
4013	A license is about to expire. Feature: %s, expiration date: %s.	Used when a license is about to expire to indicate the feature activated by the license and the expiration date of the license
4014	A license has expired. Feature: %s, expiration date: %s.	Used when a license has expired to indicate the feature activated by the license and the expiration date of the license
4015	Container limit exceeded (container depth)	Used when the specified maximum number of nested levels to be decomposed for scanning is exceeded
4016	Container limit exceeded (extract time)	Used when the specified maximum amount of time that is spent decomposing a container file and its contents is exceeded
4017	Container limit exceeded (file size)	Used when the specified maximum file size for individual files in a container file is exceeded
4018	A container limit violation has been detected.	Used when a container limit violation has occurred
4019	An error occurred while trying to replace an infected file with the repaired copy. File:	Used when an error occurs in replacing an infected file with the repaired copy to indicate the file name

Editing the ICAP access denied message

When ICAP is being used, the Symantec AntiVirus Scan Engine displays an HTML text message to a user when a requested file is blocked. (Access to a file is blocked when the file contains a virus and cannot be repaired.) The default text indicates that access is denied because the file contained a virus.

For Solaris and Linux, the default location and file name of the HTML file is /opt/SYMCScan/etc/symcsinf.htm. For Windows 2000 Server/Advanced Server, the default location and file name of the file is C:\Program Files\Symantec\Scan Engine\SYMCSINF.htm.

You can customize the text that is displayed in one of two ways:

- Edit the ICAP access denied HTML file.
- Specify an alternate HTML file.
  See "Configuring ICAP" on page 61.

The default text that is contained in the ICAP access denied message is described in Table 9-5.

Table 9-5 Default text for ICAP access denied message

Default text	Description
The page or file you just requested had a virus and was blocked by the Symantec AntiVirus Scan Engine	Text contained in the symcsinf.htm file, which is displayed to the user when a requested file contains a virus and cannot be repaired

To edit the ICAP access denied message

1. Locate the Symantec AntiVirus Scan Engine ICAP access denied HTML file and open it with a text editor.
2. Make your changes to the file.
3. Save the file.
4. Stop and restart the Symantec AntiVirus Scan Engine.

Chapter 10

Integrating the Symantec AntiVirus Scan Engine with SESA

This chapter includes the following topics:

- About SESA
- Configuring logging to SESA
- Scan engine events that are forwarded to SESA
- Interpreting scan engine events in SESA
- Uninstalling the SESA integration components
- Uninstalling the local SESA Agent

About SESA

In addition to standard local logging for the Symantec AntiVirus Scan Engine, you can also choose to log virus-related events to the Symantec Enterprise Security Architecture (SESA). SESA is an underlying software infrastructure and a common user interface framework. It integrates multiple Symantec Enterprise Security products and third-party products to provide a central point of control of security within an organization. It provides a common management framework for SESA-enabled security products, such as the Symantec AntiVirus Scan Engine, that protect your IT infrastructure from malicious code, intrusions, and blended threats.

SESA helps you increase your organization's security posture by simplifying the task of monitoring and managing the multitude of security-related events and products that exist in today's corporate environments. SESA includes an event management system that employs data collection services for events generated on computers that are managed by Symantec security products. The event categories and classes include antivirus, content filtering, network security, and systems management. The range of events varies depending on the Symantec applications that are installed and managed by SESA.

You can monitor and manage these security-related events through the SESA Console. The SESA Console is the common user interface that provides manageable integration of security technologies (Symantec or otherwise), Symantec Security Services, and Symantec Security Response. You can query, filter, and sort data to reduce the security-related events that you see through the SESA Console, which allows you to focus on threats that require your attention. You can configure alert notifications in response to events, and generate, save, and print tabular and graphical reports of event status, based on filtered views that you have created.

The Symantec Enterprise Security Architecture is purchased and installed separately. SESA must be installed and working properly before you configure the Symantec AntiVirus Scan Engine to log events to SESA.

For more information, see the SESA documentation.

Configuring logging to SESA

The logging of virus-related events to the Symantec Enterprise Security Architecture (SESA) is in addition to the standard local logging features for the Symantec AntiVirus Scan Engine. Logging to SESA is activated independently of standard local logging. If you have purchased SESA, you can choose to send a subset of the virus-related events logged by the scan engine to SESA.

See "Scan engine events that are forwarded to SESA" on page 154.

To configure logging to SESA, you must complete the following steps:

- Configure SESA to recognize the Symantec AntiVirus Scan Engine. In order for SESA to receive events from the scan engine, you must run the SESA Integration Wizard that is specific to the Symantec AntiVirus Scan Engine on each computer that is running the SESA Manager. The SESA Integration Wizard installs the appropriate integration components for identifying the individual security product (in this case, the Symantec AntiVirus Scan Engine) to SESA.

  See "Configuring SESA to recognize the Symantec AntiVirus Scan Engine" on page 147.

- Install a local SESA Agent on the computer that is running the Symantec AntiVirus Scan Engine. The local SESA Agent handles the communication between the scan engine and SESA.

  See "Installing the local SESA Agent" on page 149.

- Configure the Symantec AntiVirus Scan Engine (through the scan engine administrative interface) to communicate with the local SESA Agent and to log virus-related events to SESA.

  See "Configuring the scan engine to log events to SESA" on page 153.

Configuring SESA to recognize the Symantec AntiVirus Scan Engine

To configure SESA to receive events from the Symantec AntiVirus Scan Engine, run the SESA Integration Wizard that is specific to the Symantec AntiVirus Scan Engine on each computer that is running the SESA Manager. The SESA Integration Wizard installs the appropriate integration components for identifying the Symantec AntiVirus Scan Engine to SESA. You must run the SESA Integration Wizard for each SESA Manager computer to which you are forwarding events from the Symantec AntiVirus Scan Engine.

Each product that interfaces with SESA has a unique set of integration components. The integration components for all products that interface with SESA are available when you purchase SESA and are not distributed with the individual security products. Thus, the SESA Integration component is not part of the Symantec AntiVirus Scan Engine software distribution package.

To configure SESA to recognize the Symantec AntiVirus Scan Engine

1. On the computer on which the SESA Manager is installed, insert the SEM AV CD into the CD-ROM drive.
2. At the command prompt, change directories on the CD to the SAVSE Directory.
3. At the command prompt, type:
   java -jar setup.jar
   The SESA Integration Wizard starts.
4. Click **Next** until you see the SESA Domain Administrator Information window.
5. In the SESA Domain Administrator Information window, type the specific information about the SESA Domain Administrator and the SESA Directory.

SESA Domain Administrator Name	The name of the SESA Directory Domain Administrator account.
SESA Domain Administrator Password	The password for the SESA Directory Domain Administrator account.
IP Address of SESA Directory	The IP address of the computer on which the SESA Directory is installed (may be the same as the SESA Manager IP address if both are installed on the same computer). If you are using authenticated SSL instead of SESA default, anonymous SSL, you must enter the host name of the SESA Directory computer. For example, mycomputer.com. For more information on SESA default, anonymous SSL and upgrading to authenticated SSL, see the *Symantec Enterprise Security Architecture Installation Guide*.
SSL Port	The number of the SESA Directory secure port. The default port number is 636.

6 Follow the on-screen instructions to install the appropriate SESA integration components and complete the SESA Integration Wizard.

7 Repeat steps 1 through 6 on each SESA Manager computer to which you are forwarding Symantec AntiVirus Scan Engine events.

Installing the local SESA Agent

The local SESA Agent handles the communication between the Symantec AntiVirus Scan Engine and SESA and is installed on the same computer that is running the Symantec AntiVirus Scan Engine. The local SESA Agent is provided as part of the software distribution package for the Symantec AntiVirus Scan Engine. You have the option to install the local SESA Agent at the same time you install the scan engine or you can install the Agent at a later date. If you install the Agent at a later date, a separate install package for installing only the Agent, agentinstaller, is located in the SESA_agent directory on the distribution CD for the Symantec AntiVirus Scan Engine.

If you have more than one SESA-enabled product installed on a single computer, these products can share a local SESA Agent. However, each product must register with the Agent. Thus, even if an Agent has already been installed on the computer for another SESA-enabled security product, you must run the installer to register the Symantec AntiVirus Scan Engine with the Agent.

The local SESA Agent is preconfigured to listen on the IP address 127.0.0.1 and port number 8086. The scan engine uses this information to communicate with the Agent. If you must change the IP address or port number for the Agent, you must do so through the SESA Console. (Once an Agent is installed it is controlled through the SESA Console, even though it is running on the computer that is running the security product.) You must also update, through the Symantec AntiVirus Scan Engine administrative interface, the information that the scan engine uses to contact the local SESA Agent.

See the SESA documentation for more information.

See "Configuring the scan engine to log events to SESA" on page 153.

To install the local SESA Agent on Windows 2000 Server/Advanced Server

1. Log on to the computer on which you have installed the Symantec AntiVirus Scan Engine as administrator or with administrator rights.
2. Copy the agentinstaller.exe file from the Symantec AntiVirus Scan Engine distribution CD onto the computer.
3. Run the .exe file.
4. Indicate that you agree with the terms of the Symantec license agreement, then click **Next**.

   If you indicate No, the installation is aborted.
5. Select the Symantec AntiVirus Scan Engine from the list of products to register with SESA.

   Note: You can register only one product at a time. If you are installing the local SESA Agent to work with more than one Symantec product, you must run the installer again for each product.
6. Select the location in which to install the local Agent, then click **Next**.

   The default location is C:\Program Files\Symantec\SESA.
7. In the Primary SESA Manager IP address or host name box, type the IP address or host name of the computer on which the primary SESA Manager is running.

   If SESA is configured to use Anonymous SSL (the default setting), type the IP address of the primary SESA Manager. If SESA is configured to use Authenticated SSL, type the host name of the primary SESA Manager (for example, computer.company.com).
8. In the Primary SESA Manager port number box, type the port number on which the SESA Manager listens.

   The default port number is 443.
9. If you are running a Secondary SESA Manager that is to receive events from the scan engine, do the following:
   - In the Secondary SESA Manager IP address or host name box, type the IP address or host name of the computer on which the Secondary SESA Manager is running.
   - In the Secondary SESA Manager port number box, type the port number on which the Secondary SESA Manager listens.

     The default port number is 443.

10 In the Organizational unit distinguished name box, type the organizational unit distinguished name to which the Agent will belong.

   If the organizational unit is unknown or not yet configured, this setting can be left blank. Use the format shown in the example:

   ou=Europe,ou=Locations,dc=SES,o=symc_ses

   The domain(s) (dc=) portion of the path should correspond to the domain that is managed by the selected SESA Management Server.

11 Indicate whether the local SESA Agent should start automatically whenever the computer is restarted.

   If you indicate Demand (rather than Automatic), you must manually restart the local SESA Agent each time the computer is restarted.

12 Indicate whether the local SESA Agent should start immediately after the installation finishes.

   If you indicate No, you must manually start the local SESA Agent after the installation is complete.

The installer proceeds from this point with the installation. When the installation is complete, the Agent is installed as a Windows 2000 service, and is listed as SESA AgentStart Service in the Services Control Panel.

To install the local SESA Agent on Solaris and Linux

1 Log on as root to the computer on which you have installed the Symantec AntiVirus Scan Engine.

2 Copy the agentinstaller.sh file from the Symantec AntiVirus Scan Engine distribution CD onto the computer.

3 Change directories to the location in which you copied the file.

4 Type the following command, then press **Enter**:

   sh ./agentinstaller.sh

5 Indicate that you agree with the terms of the Symantec license agreement, then press **Enter**.

   If you indicate No, the installation is aborted.

6 Select the Symantec AntiVirus Scan Engine from the list of products to register with SESA.

Note: You can register only one product at a time. If you are installing the Agent to work with more than one Symantec product, you must run the installer again for each product.

---

7. Select the location in which to install the local SESA Agent, then click **Next**.
   The default location is /opt/Symantec/SESA.
8. Type the IP address or host name of the computer on which the primary SESA Manager is running.
   If SESA is configured to use Anonymous SSL (the default setting), type the IP address of the primary SESA Manager. If SESA is configured to use Authenticated SSL, type the host name of the primary SESA Manager (for example, computer.company.com).
9. Type the port number on which the SESA Manager listens.
   The default port number is 443.
10. If you are running a Secondary SESA Manager that is to receive events from the scan engine, do the following:
    - Type the IP address or host name of the computer on which the Secondary SESA Manager is running.
    - Type the port number on which the Secondary SESA Manager listens.
      The default port number is 443.
11. Type the organizational unit distinguished name to which the Agent will belong.
    If the organizational unit is unknown or not yet configured, this setting can be left blank. Use the format shown in the example:
    ou=Europe,ou=Locations,dc=SES,o=symc_ses
    The domain(s) (dc=) portion of the path should correspond to the domain that is managed by the selected SESA Management Server.
12. Type one of the following to indicate when the local SESA Agent should start:
    - Auto: The local SESA Agent starts automatically whenever the computer is restarted.
    - Demand: You must manually restart the local SESA Agent each time the computer is restarted.
13. Type one of the following to indicate whether the local SESA Agent should start immediately after the installation finishes:
    - 0: You must manually start the local SESA Agent after the installation is complete.
    - 1: The local SESA Agent starts immediately after the installation is complete.

The installer proceeds from this point with the installation. Unless you indicated otherwise during the installation, the local SESA Agent starts automatically when the installation is complete.

Stopping and restarting the local SESA Agent service

You may need to stop and restart the local SESA Agent.

To stop and restart the local SESA Agent service

Instructions for stopping and restarting the local service differ depending on the operating system that you are running. For Windows 2000 Server/Advanced Server, you can stop and start the service in the Services Control Panel.

To stop and restart the local SESA Agent service on Solaris

- At the command prompt, do one of the following:
  - To stop the service, type the following command:
    /etc/init.d/sesagentd stop
  - To start the service, type the following command:
    /etc/init.d/sesagentd start
  - To stop and immediately restart the service, type the following command:
    /etc/init.d/sesagentd restart

To stop and restart the local SESA Agent service on Linux

- At the command prompt, do one of the following:
  - To stop the service, type the following command:
    /etc/rc.d/init.d/sesagentd stop
  - To start the service, type the following command:
    /etc/rc.d/init.d/sesagentd start
  - To stop and immediately restart the service, type the following command:
    /etc/rc.d/init.d/sesagentd restart

Configuring the scan engine to log events to SESA

After you have installed the local SESA Agent to handle communication between the Symantec AntiVirus Scan Engine and SESA, you must configure the Symantec AntiVirus Scan Engine to communicate with the Agent by specifying the IP address and port number on which the Agent listens, and you must ensure that logging to SESA has been activated. These settings are located on the Symantec AntiVirus Scan Engine administrative interface.

To configure the scan engine to log events to SESA

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Logging tab, under Symantec Enterprise Security Architecture, check **Log events to SESA**.
3. In the SESA agent IP address box, type the IP address on which the local SESA Agent listens.

   The default setting is 127.0.0.1 (the loopback interface), which restricts connections to the same computer.
4. In the Port number box, type the TCP/IP port number on which the local SESA Agent listens.

   The port number you enter here must match the port number on which the local SESA Agent listens. The default port is 8086.
5. Click **Confirm Changes** to save the configuration.
6. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.

     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
   - Click **Save/No Restart** to save your changes (changes will not take effect until the service is restarted).

Scan engine events that are forwarded to SESA

The events that are logged to SESA are a subset of the events that are normally logged by the Symantec AntiVirus Scan Engine. The list of events that is forwarded to SESA is predefined and cannot be changed. When you activate logging to SESA, only the predefined events are forwarded, regardless of the events that you have activated for local logging purposes. However, in order for an event to be forwarded to SESA, you must also activate local logging for that event.

See "Specifying what to log" on page 112.

Table 10-1 lists the Symantec AntiVirus Scan Engine events that are forwarded to SESA when logging to SESA is activated.

Table 10-1 Individual events that are logged to SESA

Logging option	Description
Infection found	Logs all infections found in scanned files
Non-repairable infection found	Logs all infections found that cannot be repaired **Note:** When the Symantec AntiVirus Scan Engine is set to Scan Only, this log entry is generated for any infection found.
Server start	Logs all instances of scan engine startup
Server stop	Logs all instances of scan engine shutdown
Virus definition update	Logs all instances of scan engine virus definitions updates

Interpreting scan engine events in SESA

SESA provides extensive event management capabilities. SESA provides common logging of normalized event data for SESA-enabled security products like the Symantec AntiVirus Scan Engine. The event categories and classes include antivirus, content filtering, network security, and systems management. SESA also provides centralized reporting capabilities, including graphical reports. Currently, the events forwarded to SESA by the Symantec AntiVirus Scan Engine take advantage of the existing SESA infrastructure for antivirus-related events.

You can create alert notifications for certain events, including those generated by the Symantec AntiVirus Scan Engine. Notifications include pagers, SNMP traps, email, and OS Event Logs. You can define the notification recipients, day and time ranges when specific recipients are notified, and custom data to accompany the notification messages.

For more information on interpreting events in SESA and on SESA's event management capabilities, see the SESA documentation.

Uninstalling the SESA integration components

If the Symantec AntiVirus Scan Engine is no longer forwarding messages to SESA, you can uninstall the SESA Integration components from each computer that is running the SESA Manager.

To uninstall the SESA Integration components

- On the taskbar, click **Start** > **Run,** then type:
  java -jar setup.jar -uninstall

Uninstalling the local SESA Agent

The local SESA Agent is automatically uninstalled when you uninstall the Symantec AntiVirus Scan Engine. If more than one product is using the Agent, the uninstall script will remove only the Symantec AntiVirus Scan Engine registration and leave the Agent in place. If no other security products are using the Agent, the uninstall script will uninstall the Agent as well.

Appendix A

Editing the configuration file

This chapter includes the following topics:

- Editing the Symantec AntiVirus Scan Engine configuration file
- Configuration options

Editing the Symantec AntiVirus Scan Engine configuration file

In addition to using the Web-based administrative interface, you can change the Symantec AntiVirus Scan Engine settings by editing the configuration file, symcscan.cfg.

The configuration options for the Symantec AntiVirus Scan Engine can be configured through the Web-based administrative interface. Under regular circumstances, you should not need to edit the configuration file.

For Solaris and Linux, the default location for the configuration file is /opt/SYMCScan/etc/symcscan.cfg. For Windows 2000 Server/Advanced Server, the default location for the configuration file is C:\Program Files\Symantec\Scan Engine\symcscan.cfg.

Note: In editing the configuration file, all high-ASCII and double-byte characters must be written in UTF-8 encoding.

To edit the Symantec AntiVirus Scan Engine configuration file

1. Locate the Symantec AntiVirus Scan Engine configuration file.
   If you are running more than one copy of the Symantec AntiVirus Scan Engine on a computer, make sure that you have the appropriate configuration file.
2. Open the configuration file with a text editor.
3. Make your changes to the configuration file.
   See "Configuration options" on page 159.
4. Save the file.
5. Stop and restart the Symantec AntiVirus Scan Engine.

Configuration options

The configuration options are grouped according to their appearance on the interface rather than the order in which they appear in the configuration file.

Warning: Several configuration options in the configuration file are not discussed in this chapter and should not be changed. Changing these options can detrimentally affect product performance. For example, the installation directory (InstallDir) is specified at installation, and the product will not function if you change this value in the configuration file.

Changing protocol-specific settings via the configuration file

You can change the communication protocol that the scan engine uses to communicate with client applications for which it is providing scanning services.

After you select the appropriate protocol, you must provide protocol-specific configuration information. The configuration options differ depending on the protocol that you select.

See "Selecting the communication protocol" on page 58.

Changing the communication protocol

You can change the communication protocol that the scan engine uses to communicate with the client applications.

To change the communication protocol

- At Protocol=, type one of the following:
  - NATIVE: Use the native protocol.
  - ICAP: Use ICAP.
  - RPC: Use RPC.

Specifying a bind address and port number

The Symantec AntiVirus Scan Engine binds to an IP address and port number. By default, the Symantec AntiVirus Scan Engine binds to all interfaces. You can restrict access to a specific interface by entering the appropriate bind address. The default port number setting for the native protocol is port 7777. The default port number setting for ICAP is port 1344.

Note: This setting is applicable to the native protocol and ICAP.

To specify a bind address and port number

1. At BindAddress=, type the IP address on which the Symantec AntiVirus Scan Engine listens.

   Use 127.0.0.1 (the loopback interface) to let only clients that are running on the same computer connect to the Symantec AntiVirus Scan Engine.

2. At Port=, replace the existing port number with the new number.

   If you change the port number, use a number that is greater than 1024 that is not in use by any other program or service.

Specifying a directory for local file scanning

You only need to provide a local scan directory when you are using local file scanning options and you want to limit the Symantec AntiVirus Scan Engine so that only files under a particular directory can be scanned. If a local scan directory is not specified (this is the default), any file can be scanned.

To specify a directory for local file scanning

- At LocalScanDir=, type the appropriate directory structure.

  The specified directory must already exist.

Configuring ICAP via the configuration file

If you select ICAP as the protocol to be used by the Symantec AntiVirus Scan Engine, you must configure several ICAP-specific options.

To configure ICAP via the configuration file

1. At ICAPInfectionHTMLFile=, replace the existing path and file name with a new path and file name, if necessary.

   The Symantec AntiVirus Scan Engine includes a default HTML message to display to users when access to a file is denied because it contains a virus. You can customize this message by specifying an alternate path and file name or by editing the existing file. If you choose to edit the existing file, you do not have to change this setting.

2. At ICAPActionPolicy=, type one of the following to specify how to handle infected files:

   - SCAN: Deny access to the infected file (but do nothing to the infected file).
   - SCANDELETE: Delete all infected files without attempting repairs.
   - SCANREPAIR: Attempt to repair infected files (but do nothing to files that cannot be repaired).
   - SCANREPAIRDELETE: Attempt to repair infected files, and delete any unrepairable files from archive files.

3. At ICAPResponse=, type one of the following to specify the scan engine response when a file is blocked because it is unrepairable (ICAP 1.0 only):

   - 0: Send an ICAP 403 response.
   - 1: Send a replacement file.

   Depending on the ICAP 1.0 application for which the scan engine is providing scan and repair services, you may need to adjust this setting. The default setting is to send a replacement file (the file specified for ICAPInfectionHTMLfile) when a file is blocked because it is unrepairable. However, some ICAP 1.0 applications are configured to receive the ICAP 403 response instead.

Configuring RPC via the configuration file

If you select RPC as the protocol to be used by the Symantec AntiVirus Scan Engine, you must configure several RPC-specific options.

To configure RPC via the configuration file

1. At RPCClient=, type the IP address for each RPC client for which the Symantec AntiVirus Scan Engine is to provide scanning services.

   Use the format <IPaddress>;<IPaddress>;<IPaddress>, where <IPaddress> is a single IP address for a supported RPC client.

2. At RPCActionPolicy=, type one of the following to specify how to handle infected files:

   - SCAN: Deny access to the infected file (but do nothing to the infected file).
   - SCANREPAIR: Attempt to repair infected files (but do nothing to files that cannot be repaired).
   - SCANREPAIRDELETE: Attempt to repair infected files, and delete any unrepairable files from archive files.

3. At RPCConnectionCheckInterval=, type (in seconds) the interval at which the Symantec AntiVirus Scan Engine checks to ensure that the connection to the RPC client is still active.

   The default interval is 20 seconds.

4. At RPCMaxReconnectAttempts=, type the maximum number of attempts the Symantec AntiVirus Scan Engine will make to reestablish a lost connection to the RPC client.

   The default setting is 0, which causes the Symantec AntiVirus Scan Engine to try indefinitely to reestablish a connection.

Quarantining unrepairable infected files

When you are using the RPC protocol, you can quarantine unrepairable infected files using the Symantec Central Quarantine. The Symantec Central Quarantine software is included on the Symantec AntiVirus Scan Engine distribution CD. The Symantec AntiVirus Scan Engine forwards infected items that cannot be repaired to the Symantec Central Quarantine. Typically, heuristically detected viruses that cannot be eliminated by the current set of virus definitions are forwarded to the Quarantine and isolated so that the viruses cannot spread.

See "Quarantining unrepairable infected files" on page 70.

To quarantine unrepairable infected files

1. At QuarantineInUse=, type **1** to quarantine unrepairable infected files.
   The default setting is 0 (files are not quarantined).
2. At QuarantineServer=, type the host name or the IP address for the computer on which the Symantec Quarantine Server is installed.
3. At QuarantinePort, type the TCP/IP port number to be used by the Symantec AntiVirus Scan Engine to pass files to the Central Quarantine.
   This setting must match the port number that is selected at installation for the Symantec Quarantine Server.

Changing resource allocation via the configuration file

You can change basic configuration options for the operation of the Symantec AntiVirus Scan Engine.

See "Allocating resources" on page 72.

Changing the temp directory location

The Symantec AntiVirus Scan Engine must store files in a temporary directory for virus scanning. To support sites with large, specialized disk configuration, the location of this temporary directory can be specified. The default temporary directory for Linux and Solaris is /tmp/navtemp. The default temporary directory for Windows 2000 Server/Advanced Server is determined at installation.

To specify a different location for the temporary directory

- At TempDir=, replace the existing path with the new path.

Changing the number of scan threads

You can select the number of scan threads that are available for concurrent scanning.

To change the number of scan threads

- At ScanThreads=, replace the existing number of scan threads with the new number.
  The default number of threads is 16.

Changing the threshold number of queued requests

When the number of queued requests to the Symantec AntiVirus Scan Engine exceeds the specified threshold, the scan engine is at maximum load.

To change the threshold number of queued requests to the Symantec AntiVirus Scan Engine

- At LoadMaximumQueuedClients=, type the maximum number of queued requests.

  The default setting is 100.

Specifying an alert interval

The alert interval is the number of minutes between log entries or alerts generated to indicate that maximum load has been exceeded.

To change the alert interval

- At LoadExceededAlertInterval=, replace the existing interval with the new interval.

  The default setting is five minutes.

Changing the virus definition product name

If you are running more than one scan engine on a single computer, the product name must be unique for each service so that both scan engines receive updated virus definitions via LiveUpdate. This option is applicable only if you are running the scan engine on Solaris or Linux.

To change the virus definition product name

- At DefinitionProductName=, type the new virus definition product name.

Limiting resources for in-memory file processing

You can limit the resources that are consumed for in-memory file processing by specifying the maximum amount of RAM (in bytes) to be used for the in-memory file system and the maximum file size (in bytes) that can be stored in the in-memory file system.

To limit resources for in-memory file processing

1 At InMemoryFileSystemSize=, type the maximum amount of RAM that can be used for the in-memory file system.

The default setting is 16000000 (~16 MB).

2 At MaxInMemoryFileSize=, type the maximum file size that can be stored in the in-memory file system.

Files that exceed the specified size are written to disk. The default setting is 3000000 (~3 MB).

Configuring logging options via the configuration file

You can activate logging for selected scan engine activities and change the location of log files.

See "Configuring standard logging" on page 111.

Specifying a different location for the log files

To accommodate sites with specialized disk configuration, the location of the Symantec AntiVirus Scan Engine log files can be changed (Solaris and Linux only).

To specify a different location for the log files

- At LogDir=, replace the existing location with the new location.

Specifying what to log

The Symantec AntiVirus Scan Engine can be configured to log a variety of events. Standard logging for the Symantec AntiVirus Scan Engine is divided into three categories of events to be logged: errors, warnings, and information. You can enable logging for an entire category or you can selectively enable logging for only certain events. Logging for all errors and warnings is enabled by default.

In the configuration file, the options for logging are:

- LOGAllErrorsEnable=
- LOGAllWarningsEnable=
- LOGAllInfoEnable=
- LOGCrashAlertEnable=
- LOGDefErrorAlertEnable=
- LOGLoadExceededAlertEnable=

- LOGSNMPSMTPAlertEnable=
- LOGLicenseExpired=
- LOGInfectionAlertEnable=
- LOGNonRepairableInfectionAlertEnable=
- LOGLicenseAboutExpired=
- LOGStartUpAlertEnable=
- LOGShutDownAlertEnable=
- LOGDefUpdateAlertEnable=
- LOGFileScanAlertEnable=

To specify what to log

- At each logging option shown in the configuration file, type one of the following:
  - 1: Activate the logging option.
  - 0: Deactivate the logging option.

Changing the location and file name of the message string file

The message text for Symantec AntiVirus Scan Engine alert messages, log entries, and SMTP insert messages is contained in an ASCII text file. You can change the location and file name of this file.

To change the path and file name of the message string file

- At StringFile=, replace the existing path and file name with a new path and file name.

Configuring the scan engine to log events to SESA

If you are running the Symantec Enterprise Security Architecture (SESA), you must configure the Symantec AntiVirus Scan Engine to communicate with the local Agent by specifying the IP address and port number on which the Agent listens, and you must ensure that logging to SESA has been activated.

See "Integrating the Symantec AntiVirus Scan Engine with SESA" on page 145.

To configure the scan engine to log events to SESA

1. At LogSESA, type **1** to log events to SESA.
   The default setting is 0 (events are not logged to SESA).
2. At SESAIP, type the IP address on which the local SESA Agent listens.
   The default setting is 127.0.0.1 (the loopback interface), which restricts connections to the same computer.
3. At SESAPort, type the TCP/IP port number on which the local SESA Agent listens.
   The port number that you enter here must match the port number on which the SESA Agent listens. The default setting is port 8086.

Configuring alerting via the configuration file

You can activate SNMP and SMTP alerting by providing the information for delivery of the alerts and selecting the specific activities for which you want to receive alerts.

See "Activating alerts" on page 77.

Activating SNMP alerting via the configuration file

In the configuration file, the SNMP alerting options are:

- SNMPPrimary=
- SNMPSecondary=
- SNMPCommunityString=
- SNMPCrashAlertEnable=
- SNMPDefErrorAlertEnable=
- SNMPLoadExceededAlertEnable=
- SNMPInfectionAlertEnable=
- SNMPNonRepairableInfectionAlertEnable=
- SNMPStartUpAlertEnable=
- SNMPShutDownAlertEnable=
- SNMPDefUpdateAlertEnable=
- SNMPLicenseAboutExpired=
- SNMPLicenseExpired=

To activate SNMP alerting via the configuration file

1. At SNMPPrimary=, type the IP address of the primary SNMP console that will receive alerts.
2. At SNMPSecondary=, type the IP address of a secondary SNMP console that will receive alerts.
   You do not have to specify a secondary SNMP console.
3. At SNMPCommunityString=, type the SNMP community string.
   The default setting is public.
4. At each alert option in the configuration file, type one of the following:
   - 1: Activate the alert.
   - 0: Deactivate the alert.

Activating SMTP alerting via the configuration file

In the configuration file, the SMTP alerting options are:

- SMTPPrimary=
- SMTPSecondary=
- SMTPCrashAlertEnable=
- SMTPDefErrorAlertEnable=
- SMTPLoadExceededAlertEnable=
- SMTPInfectionAlertEnable=
- SMTPNonRepairableInfectionAlertEnable=
- SMTPStartUpAlertEnable=
- SMTPShutDownAlertEnable=
- SMTPDefUpdateAlertEnable=
- SMTPLicenseAboutExpired=
- SMTPLicenseExpired=
- SMTPRecipList=
- SMTPDomain=

To activate SMTP alerting via the configuration file

1. At SMTPPrimary=, type the IP address of the primary SMTP server that will forward alerts.
2. At SMTPSecondary=, type the IP address of a secondary SMTP server that will forward alerts if communication with the primary SMTP server fails.

   You do not have to specify a secondary SMTP server.
3. At each alert option in the configuration file, type one of the following:
   - 1: Activate the alert.
   - 0: Deactivate the alert.
4. At SMTPRecipList=, type the email addresses for the recipients of SMTP alerts.

   Separate multiple addresses with a comma or space.
5. At SMTPDomain=, type the local domain for the Symantec AntiVirus Scan Engine.

   The domain name is added to the From field for SMTP alert messages, so that SMTP alert messages that are generated by the Symantec AntiVirus Scan Engine originate from ScanServer@<servername>.<domainname>, where <servername> is the name of the computer that is running the Symantec AntiVirus Scan Engine and <domainname> is the SMTPDomain that you supply here.

Changing the administration settings via the configuration file

You can configure settings for the Symantec AntiVirus Scan Engine administrative interface and the virtual administrator account.

See "Changing the administration settings" on page 47.

Specifying a bind address and port number for the administrative interface

The administrative interface binds to an IP address and port number. By default, this Web interface binds to all interfaces. You can restrict access to a specific interface by entering the appropriate bind address. The default port number is 8004.

To specify a bind address and port number for the administrative interface

1. At AdminBindAddress=, type the IP address on which the Web interface listens.
2. At AdminPort=, replace the existing port number with the new number.
   If you change the port number, use a number that is greater than 1024 that is not in use by any other program or service. If the port number is not set, the interface is not enabled.

Clearing the password for the administrator account

The Symantec AntiVirus Scan Engine is managed using a virtual administrative account. You are prompted to provide a password for this account at installation. The password for this account can be changed at any time through the Symantec AntiVirus Scan Engine administrative interface.

Note: You cannot change the password via the configuration file because the password is encrypted in the configuration file. If you forget the password for the virtual administrative account, clear the AdminPassword variable in the configuration file, and then log on to the administrative interface (you won't need a password) to enter a new password.

To clear the password for the administrator account

- At AdminPassword=, delete the encrypted password.

Changing the administrator timeout period

The Symantec AntiVirus Scan Engine is configured by default to automatically log off the administrator after a selected period of inactivity. The default period of inactivity is five minutes (300 seconds). You can change the default timeout period.

To change the administrator timeout period

- At AdminPortTimeout=, type the amount of time (in seconds) after which the Symantec AntiVirus Scan Engine automatically logs off the administrator.

Specifying processing limits via the configuration file

You can impose restrictions on the amount of resources that can be used to handle individual files. These processing limits can be used to help you manage your resources and to protect your network against denial of service attacks.

See "Specifying processing limits" on page 87.

To specify processing limits

You can specify processing limits that apply to the following:

- Large container files: You can set limits to control the resources expended on large container files.
- All files: Other types of limits can be applied to all files, such as the maximum number of bytes to be read in determining whether a file is MIME-encoded.

To specify processing limits for large container files via the configuration file

1. At MaxExtractTime=, do one of the following:
   - Type the maximum allowable amount of time, in seconds, for decomposing a container file and its contents.
   - Type **0** to disable this variable.

   The default setting is 180 seconds (3 minutes).
2. At MaxExtractSize=, do one of the following:
   - Type the maximum allowable file size, in bytes, for each file within a container file to be decomposed.
   - Type **0** to disable this variable.

   The default setting is 100 MB.
3. At MaxExtractDepth=, do one of the following:
   - Type the maximum allowable number of nested levels of files within a container file to be handled by the decomposer.
   - Type **0** to disable this variable.

   The default setting is 10 levels.

4 At LimitChoiceStopCont=, type one of the following:

- 0: Allow access to container files for which one or more limits are exceeded.
- 1: Deny access to container files for which one or more limits are exceeded. This is the default setting.

5 At RejectMalformedContainers=, type one of the following:

- 0: Allow access to all malformed containers.
- 1: Deny access if container type cannot be identified.
  This is the default setting.
- 2: Deny access to all malformed containers.

To specify processing limits that apply to all files via the configuration file

1 At MaxFileNameLength=, do one of the following:

- Type the maximum allowable file name length, in bytes, for a given file.
- Type **0** to disable this variable.

The default setting is 1024 bytes.

Note: This feature is functional for the native protocol only.

---

2 At NonMIMEThreshold=, type the maximum number of bytes that can be read to determine whether a file is MIME-encoded.
The default setting is 200000 bytes.

Changing the antivirus settings via the configuration file

You can configure certain aspects of antivirus scanning, including specifying file types to be scanned.

See "Configuring antivirus settings" on page 92.

Changing the Bloodhound sensitivity level

To supplement the detection of virus infections by virus signature, the Symantec AntiVirus Scan Engine includes the Symantec patented Bloodhound technology, which heuristically detects new or unknown viruses. The sensitivity of the Bloodhound technology can be adjusted.

To change the Bloodhound sensitivity level

- At BloodhoundLevel=, type one of the following:
  - 1: Low sensitivity
  - 2: Medium sensitivity
  - 3: High sensitivity
  - 0: Off

Specifying which file types to scan

Viruses are found only in file types that contain executable code. Bandwidth and time can be saved by limiting the files to be scanned to only those file types that can contain viruses. You can control which file types are scanned by specifying those extensions that you do not want to scan (using an exclusion list) or by specifying those extensions that you want to scan (using an inclusion list), or you can scan all file types regardless of extension.

To specify which file types to scan

The default exclusion list is preconfigured to contain the file extensions for file types that are not likely to contain viruses, but you can edit the default list. The Symantec AntiVirus Scan Engine is configured by default to scan all file types except those that are contained in the exclusion list.

To scan all files regardless of extension

- At ExtensionPolicy=, type **0**.

To scan only files with extensions that are in the inclusion list

1. At ExtensionPolicy=, type **1**.
2. Edit the ExtensionList (this is the inclusion list) to add extensions that you want to scan or delete extensions that you do not want to scan.

   Use a period with each extension in the list. Separate each extension with a semicolon (for example, .com;.doc;.bat;.foo). To scan files that have no extension, use two adjacent semicolons (for example, .com;.exe;;).

To scan all files except those with extensions that are in the exclusion list

1. At ExtensionPolicy=, type 2.
2. Edit the ExclusionList to add extensions that you do not want to scan or delete extensions that you want to scan.

   Use a period with each extension in the list. Separate each extension with a semicolon (for example, .com;.doc;.bat;.foo). To exclude files that have no extension, use two adjacent semicolons (for example, .com;.exe;;).

Blocking MIME partial message content

The Symantec AntiVirus Scan Engine must have a MIME-encoded message in its entirety to effectively scan it for viruses. Some email software applications break large messages down into a number of smaller, more manageable, partial messages for transmission. The Symantec AntiVirus Scan Engine is configured by default to reject partial messages because they cannot be effectively scanned for viruses.

To block MIME partial message content

- At RejectPartialMessages=, type one of the following:
  - 0: Block partial messages.

    This is the default setting.
  - 1: Allow access to partial messages.

Activating mail message body updates

You can add text to the bodies of MIME-encoded messages to warn recipients that a virus was found in an attachment or that an attachment was deleted because it violated the mail filter policy. The default text indicates that an attachment was infected and repaired or deleted because it could not be repaired, or that an attachment was deleted due to a mail policy violation.

See "Inserting text into MIME-encoded messages" on page 107.

To activate mail message body updates

- At UpdateMailBody=, type one of the following:
  - 1: Activate mail message body updates.
  - 0: Deactivate mail message body updates.

Scheduling LiveUpdate to occur automatically

You can schedule LiveUpdate to run automatically to obtain updated virus definitions. Scheduling LiveUpdate to occur automatically at a specified time interval ensures that the Symantec AntiVirus Scan Engine always has the most current virus definitions. You should schedule LiveUpdate so that you do not have to remember to update virus definitions regularly.

Warning: Scheduling LiveUpdate to occur automatically should be handled through the Symantec AntiVirus Scan Engine administrative interface (rather than by editing the configuration file). Entering an invalid value in the configuration file can result in LiveUpdate not functioning properly, leaving your network vulnerable to virus attack because the Symantec AntiVirus Scan Engine is not receiving updated virus definitions files.

To schedule LiveUpdate to update virus definitions automatically

- At LiveUpdateSchedule=, type the frequency at which LiveUpdate is attempted.

  Specify the desired value in seconds. For example, to schedule LiveUpdate to occur once every hour, type 3600. LiveUpdate is not scheduled by default.

Extracting all streams from OLE structured storage documents for scanning

Certain Microsoft files, such as Microsoft Word and Excel documents, are OLE (object linking and embedding) structured storage documents. OLE is a compound document standard developed by Microsoft that enables objects to be created with one application and linked or embedded in a second application. In this type of structured storage document, data is stored in a number of streams. Only certain streams typically contain content that can contain viruses. The Symantec AntiVirus Scan Engine is configured by default to extract and scan only those streams that are likely to contain viruses. For maximum protection, you can choose to extract and scan all streams, but performance may be negatively impacted depending on the number (and content) of these types of files to be scanned.

To extract and scan all streams from OLE structured storage documents

- At ExtractNativeOLEStreamsOnly=, type **0**.

  The default setting is 1, which limits scanning to only those streams that are likely to contain viruses.

Appendix B

Reviewing scanning statistics from the command line

This chapter includes the following topics:

- Using the getstat utility
- Interpreting getstat utility data

Using the getstat utility

The Symantec AntiVirus Scan Engine maintains scanning statistics so that Internet service providers can bill for antivirus scanning based on several billing schemes. Each time that a file is scanned, the Symantec AntiVirus Scan Engine submits scan statistics to the billing subsystem, which maintains an encrypted data file. You can access this information through the administrative interface.

See "Generating scanning statistics from the billing logs" on page 121.

You can also use the getstat utility, which is provided with the Symantec AntiVirus Scan Engine, to obtain statistics for a given date range via the command line. For Solaris and Linux, the default location for the getstat utility is /opt/SYMCScan/bin/getstat. For Windows 2000 Server/Advanced Server, the default location is C:\Program Files\Symantec\Scan Engine\getstat.

To use the getstat utility

1. Change directories to the directory in which the getstat tool is located.
2. Type a command using the following format:

   getstat.exe symcsbps.dat <endingdate> <numberofdays>

   where <endingdate> is the last day of the billing cycle (the last day in the time range for which you want information on scan engine utilization), and <numberofdays> is the number of days in the billing cycle (or the number of days for which you want to view utilization statistics). If the symcsbps.dat file is not located in the same directory as the getstat utility, you must include the path to the log file in the command as well. Use the format MM/DD/YYYY for the <endingdate> entry.

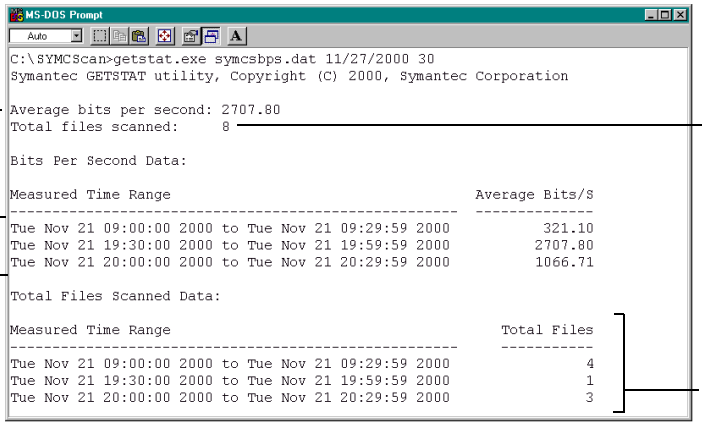
   For example, if you type

   getstat.exe symcsbps.dat 11/27/2001 30

   the generated report includes utilization information for the 30-day period ending on 11/27/01.

Interpreting getstat utility data

A sample getstat utility report is shown below.


MS-DOS Prompt
Auto
C:\SYMCScan>getstat.exe symcsbps.dat 11/27/2000 30
Symantec GETSTAT utility, Copyright (C) 2000, Symantec Corporation
Average bits per second: 2707.80
Total files scanned: 8
Bits Per Second Data:
Measured Time Range Average Bits/S
Tue Nov 21 09:00:00 2000 to Tue Nov 21 09:29:59 2000 321.10
Tue Nov 21 19:30:00 2000 to Tue Nov 21 19:59:59 2000 2707.80
Tue Nov 21 20:00:00 2000 to Tue Nov 21 20:29:59 2000 1066.71
Total Files Scanned Data:
Measured Time Range Total Files
Tue Nov 21 09:00:00 2000 to Tue Nov 21 09:29:59 2000 4
Tue Nov 21 19:30:00 2000 to Tue Nov 21 19:59:59 2000 1
Tue Nov 21 20:00:00 2000 to Tue Nov 21 20:29:59 2000 3

95th-percentile bandwidth measurement for reported period

Calculated average bps for each 30-minute period (shown in chronological order)

Total number of files that were scanned for the reported period

Number of files that were scanned for each 30-minute period (shown in chronological order)

The total number of files that were scanned should not be interpreted strictly as a physical file count. This total includes the number of files as well as additional objects within container files that were scanned. Some containers, such as MIME-encoded messages and Microsoft Office documents, have additional embedded objects that are not files but that may be scanned depending on the ExtensionList settings. The total does not include objects within container files that were not scanned because the object's extension did not match those in the ExtensionList setting.

For each 30-minute period in the specified date range, the total number of files that were scanned and the average bits per second that were scanned for that 30-minute increment are reported. The 30-minute time periods are reported in Greenwich mean time (GMT).

Appendix C

Return codes

This chapter includes the following topics:

- Native protocol return codes
- ICAP version 0.95 return codes
- ICAP version 1.0 return codes
- RPC return codes

Native protocol return codes

The following return codes are generated for the native protocol:

- 200 Command okay.
- 201 Output file available.
- 203 Local output file available.
- 220 Symantec AntiVirus Scan Engine ready.
- 221 Service closing transmission channel.
- 230 File scanned.
- 420 Service not available, closing transmission channel.
- 430 File not acceptable at this time.
- 500 Syntax error, command unrecognized.
- 501 Syntax error in parameters.
- 502 Command not implemented.
- 503 Bad sequence of commands.
- 504 Unsupported protocol version.
- 530 File not acceptable.
- 531 File unscannable.
- 532 Output file unavailable.
- 533 Error scanning file.
- 534 File name exceeds configured length.
- 535 Maximum Extract Time exceeded - scan incomplete.
- 536 Maximum Extract Depth exceeded - scan incomplete.
- 537 Maximum Extract Size exceeded - scan incomplete.
- 538 Malformed container file found. File not scanned.
- 539 Aborted - no AV scanning license.

ICAP version 0.95 return codes

The following return codes are generated for ICAP version 0.95:

- 100 Continue
- 200 OK
- 201 Created
- 204 No content necessary.
- 400 Bad request.
- 403 Forbidden. Infected and not repaired.
- 404 Not found.
- 405 Method not implemented.
- 420 Container extract time violation. File not scanned.
- 425 Container size violation. File not scanned.
- 430 Container depth violation. File not scanned.
- 431 Malformed container found. File not scanned.
- 432 Mail policy violation. File not scanned.
- 500 Internal server error.
- 503 Service unavailable/overloaded.
- 505 ICAP version not supported.
- 531 Container type cannot be repaired.
- 533 Error scanning file.
- 539 Aborted - no AV scanning license.

ICAP version 1.0 return codes

The following return codes are generated for ICAP version 1.0:

- 100 Continue
- 200 OK
- 201 Created
- 204 No content necessary.

- 400 Bad request.
- 403 Forbidden. Infected and not repaired.
- 404 Not found.
- 405 Method not implemented.
- 408 Request timeout.
- 500 Internal server error.
- 503 Service unavailable/overloaded.
- 505 ICAP version not supported.
- 533 Error scanning file.
- 539 Aborted - no AV scanning license.
- 551 Resource unavailable.

RPC return codes

The following return codes are generated for RPC:

- Infection found, repaired
- Infection found, repair failed
- Infection found, repair failed, file quarantined
- Infection found, repair failed, quarantine failed
- Infection found
- Maximum Extract Size exceeded, scan incomplete
- Maximum Extract Time exceeded, scan incomplete
- Maximum Extract Depth exceeded, scan incomplete
- Aborted - No AV scanning license
- Internal server error
- Infection found, repair failed, read-only file

Appendix D

Using the silent install feature

This chapter includes the following topics:

- About the silent install feature
- Creating the response file
- Initiating the silent install using the response file
- Using the silent install feature for uninstall

About the silent install feature

The silent install feature lets you automate the installation of the Symantec AntiVirus Scan Engine. You can use the silent install feature when you are installing multiple Symantec AntiVirus Scan Engines with identical input values for installation. The silent install feature lets you capture the required input values for installation in a response file. You can use the response file for subsequent installations to read in the values so that the installations are silent (freeing you from having to repeatedly supply input values for each installation).

Implementing the silent install feature is a two-step process:

- Create a response file to capture your input values for installation.
- Run the install program to read the response file and perform the install silently using the same responses that you specified in the response file.

Creating the response file

The response file contains the input values for the required responses for installation of the Symantec AntiVirus Scan Engine. You can create different response files for different installation scenarios, for example, different protocols, install directories, or RPC clients.

The procedures for creating the response file differ for Windows 2000 Server/ Advanced Server, Solaris, and Linux.

Creating the response file on Windows 2000 Server/Advanced Server

For Windows 2000 Server/Advanced Server, you must run the installation once to create the response file. The Symantec AntiVirus Scan Engine is initially installed with the /r switch so that your responses are captured in the response file. Ensure that the scan engine is not already installed before you begin.

To create the response file on Windows 2000 Server/Advanced Server

1. Change directories to the location of the Symantec AntiVirus Scan Engine installation program, ScanEngine.exe.
2. At the command prompt, type:

   ScanEngine /r

   The installation proceeds as a normal (non-silent) install.
3. During the installation, respond to each dialog box with the desired input value for the silent installs.

   When the installation completes, the response file is written to the disk.

Note: For Windows 2000 Server/Advanced Server only, the password that you enter for the virtual administrative account is stored in the response file unencrypted. Protect the response file accordingly to prevent the password from being compromised.

By default, the response file, setup.iss, is written to the WinNT directory. To specify a different name and location for the response file, use the /f1 switch. For example, the following command writes a response file, install_savse.iss, to the temporary directory C:\Temp:

ScanEngine /r /f1"C:\Temp\install_savse.iss"

Note: Quotes must be used around the path and file name to handle an embedded space.

Creating the response file on Solaris and Linux

For Solaris and Linux, you can create the response file before you install the Symantec AntiVirus Scan Engine.

A default response file, named response, is included as part of the Symantec AntiVirus Scan Engine software distribution package. The response file is a text file that is preconfigured to contain the default settings for the scan engine installation options. You must edit this response file so that it contains the desired input values for the silent install.

Note: Do not delete any of the parameters in the response file. The installer must read a value for each parameter.

The input values contained in the response file are listed in Table D-1.

Table D-1 Input values in the response file

Input value	Description
SCANPort	Port number on which the Symantec AntiVirus Scan Engine listens. This port number must be exclusive to the Symantec AntiVirus Scan Engine. The default port number differs depending on the protocol selected. ■ NATIVE: 7777 ■ ICAP: 1344
Protocol	Communication protocol used by the scan engine. Use NATIVE or ICAP.
AdminPort	Port number on which the Web-based administrative interface listens. The default port number is 8004.
AdminPassword	Password for the virtual administrative account that you will use to manage the Symantec AntiVirus Scan Engine. **Note:** You must use the GenEncryptPW utility, included in the scan engine distribution, to generate an encrypted password. Use the encrypted string returned by the utility for this value. See "Generating an encrypted password" on page 190.
InstallDir	Location in which to install the Symantec AntiVirus Scan Engine. The default location is /opt/SYMCScan.
LogDir	Location in which to place the Symantec AntiVirus Scan Engine log files. The default location is /var/log.
SymShared	Location of the SymShared directory. The default location is /opt/Symantec. **Note:** The SymShared directory contains the virus definitions that are used by the Symantec AntiVirus Scan Engine to scan for viruses. If you have multiple Symantec products installed on the computer, this directory lets the products share virus definitions. If you have previously installed a Symantec AntiVirus product on the computer, this directory may already exist.

Table D-1 Input values in the response file

Input value	Description
CreateAVDefsGroup	Boolean value that indicates whether to create the avdefs group. Use 0 if the group already exists, or use 1 to create the group. The avdefs group has access rights to the directory that contains the virus definitions that are used by the Symantec AntiVirus Scan Engine. If you have previously installed a Symantec product on the computer, this group may already exist.
mservip	IP address or host name of the computer on which the Symantec Enterprise Security Architecture (SESA) Manager is running. **Note:** A value for this parameter is necessary only if you plan to configure the Symantec AntiVirus Scan Engine to log events to SESA.
mserverport	Port number on which the SESA Manager listens. The default port number is 443. A value for this parameter is necessary only if you plan to configure the Symantec AntiVirus Scan Engine to log events to SESA.
LogSesa	Boolean value that indicates whether to log events to SESA. Use 0 to deactivate logging to SESA, or use 1 to activate logging to SESA.

To create the response file on Solaris and Linux

1. Locate the response file, response, on the Symantec AntiVirus Scan Engine distribution CD and copy it to the /tmp directory on the computer that you are using.

   For the silent install to initiate, the response file must be located in the /tmp directory.

2. Rename the file to no-ask-questions and open the file.

3. Supply the desired input value for each parameter.

   Changes should be made only to the right of the equal sign (=).

4 At AdminPassword=, copy and paste the encrypted string that was generated by the GenEncryptPW utility.

Make sure that you copy the encrypted string in its entirety.

See "Generating an encrypted password" on page 190.

5 Save the file.

Generating an encrypted password

The GenEncryptPW utility is included in the scan engine distribution so that you can protect the administrative password for managing the Symantec AntiVirus Scan Engine. This utility encrypts the specified password and returns an encrypted string. You must copy the encrypted string in its entirety and paste it in the appropriate location in the response file.

To generate an encrypted password

1 Locate the GenEncryptPW utility on the Symantec AntiVirus Scan Engine distribution CD and copy it to the computer that you are using.

2 At the command prompt, type **GenEncryptPW <password>**, where <password> is the password that you will use to access the Symantec AntiVirus Scan Engine administrative interface.

The utility returns an encrypted string.

3 Save the entire encrypted string that is returned by the GenEncryptPW utility.

Initiating the silent install using the response file

The procedures for initiating the silent install differ for Windows 2000 Server/ Advanced Server, Solaris, and Linux.

The silent install on Solaris and Linux initiates automatically so long as the installer finds the response file in the correct location. The existence of the no-ask-questions file in the /tmp directory tells the installer to perform a silent install using the input values contained in the file. Before you begin the install, ensure that the appropriate response file, titled no-ask-questions, is located in the /tmp directory.

To initiate a silent install on Windows 2000 Server/Advanced Server, you must run the install program with the /s switch to read the response file. The installation proceeds silently, using the input values that are contained in the response file.

Note: If you initiate a Symantec AntiVirus Scan Engine silent install in which RPC is the selected communication protocol (Windows 2000 Server/Advanced Server only), the RPC password that you enter is stored in the response file unencrypted. Protect the response file accordingly to prevent the password from being compromised.

To initiate a silent install on Windows 2000 Server/Advanced Server

1. Change directories to the location of the Symantec AntiVirus Scan Engine installation program, ScanEngine.exe.
2. At the command prompt, type:

   ScanEngine /s /f1"C:\WinNT\setup.iss"

   The above command shows the default response file, setup.iss, in its default location, the WinNT directory. You will need to substitute appropriately if you have changed the response file name and location. For example:

   ScanEngine /s /f1"C:\Temp\install_savse.iss"

   The silent install proceeds automatically from this point using the input values that are contained in the response file.

Using the silent install feature for uninstall

You also can automate the uninstall for the Symantec AntiVirus Scan Engine on Windows 2000 Server/Advanced Server. The procedures for using the silent uninstall are the same as for the silent install.

Using the silent install feature for uninstall

You must create a second response file for uninstall. After you have created the response file, you can initiate the silent uninstall by running the install program with the /s switch to read the response file.

Note: When you create the response file for the silent uninstall, use the /f1 switch to specify a different name and location for the response file (rather than allowing the default settings) so you can easily distinguish the uninstall response file from any response files that you have saved for silent install.

To create the uninstall response file

- At the command prompt, type:
  ScanEngine /r /f1"C:\Temp\ScanEngine_uninstall.iss"

To initiate the silent uninstall

- At the command prompt, type:
  ScanEngine /s /f1"C:\Temp\ScanEngine_uninstall.iss"

Index

A

administrative interface
- accessing 43
- changing settings for 47
- description of 42, 44

administrator
- password, configuring 47
- timeout, configuring 48

alert interval, configuring 73
alerts
- customizing 133
- HTML, customizing (ICAP) 143
- SMTP, configuring 80
- SNMP, configuring 77

antivirus scanning
- description of 22
- specifying file types for 92
- testing detection capabilities 25

B

billing logs
- description of 110
- generating scanning statistics from 121
- interpreting scanning statistics 123

bind address, configuring
- for administrative interface 47
- for ICAP 62
- for native protocol 59

Bloodhound sensitivity, configuring 92

C

command buttons 45
configuration file, editing 157
container file limits, specifying 87

D

denial of service attacks, protection against 87

F

file types, specifying for scanning 93
filtering email
- blocking partial messages 106
- by attachment file name 103
- by attachment file size 105
- by maximum mail size 100
- by message origin 102
- by subject 100

G

getstat utility
- interpreting data 179
- using 178

H

HTML alerts, customizing (ICAP) 143

I

ICAP
- configuring 61
- discussion of 21
- return codes 183

in-memory file processing limits, configuring 74
installing
- on Linux 35
- on Solaris, as root 32
- on Windows 2000 Server/Advanced Server 30
- preparing for 29
- silent install 185

L

licensing
- activating a license 53
- checking the license status 55
- discussion 52
- removing licenses 53
- warning and grace periods 52

Linux
- installing 35
- stopping and starting service 38, 153
- system requirements 28
- uninstalling 39

LiveUpdate
- configuring 126
- configuring a LiveUpdate server 129
- description of 126
- scheduling via the command line 128

load balancing 20
local SESA Agent, installing 149
Log All options 113
logging
- clearing logs 118
- configuring 111
- customizing log entries 141
- description of 110
- downloading logs 117
- Log All options 113
- log file location, changing 111
- obtaining summary data 120
- SESA 146

M

mail filter policy
- blocking partial messages 106
- by attachment file name 103
- by attachment file size 105
- by mail subject 100
- by maximum mail size 100
- by message origin 102
- configuring 97
- MIME augmentation 107

malformed container files, blocking access 88
message string file
- configuring location of 116
- description of 132
- editing 132

MIME augmentation
- configuring 107
- customizing message text 138

N

native protocol
- configuring 59
- discussion of 21
- return codes 182

P

partial messages, blocking 106
port number, configuring
- for administrative interface 47
- for ICAP 62
- for native protocol 59

protocol
- configuring 58
- ICAP 21
- native 20
- RPC 22

Q

quarantining infected files 70
queue size, configuring 73

R

return codes
- ICAP 0.95 183
- ICAP 1.0 183
- native protocol 182
- RPC 184

RPC
- configuring 64
- discussion of 22
- quarantining unrepairable files 70
- return codes 184

S

scanning threads, configuring 73
service startup properties, editing 69
SESA Integration Wizard, installing 147

SESA, logging to
configuring 147
configuring the scan engine 153
discussion 147
installing the local Agent 149
running the SESA Integration Wizard 147
silent install
creating the response file 186
Solaris and Linux 187
Windows 186
discussion 186
initiating the install 190
using for uninstall 191
SMTP alerting, configuring 80
SNMP alerting, configuring 77
Solaris
installing 32
stopping and starting service 37, 153
system requirements 28
uninstalling 39
starting service 37
statistics, from billing logs
interpreting 123
obtaining 121
using the getstat utility 178
Status pane 45
stopping service 37
summary log data
interpreting 121
obtaining 120
system requirements 28

T

temporary directory, specifying 72

U

uninstalling the Symantec AntiVirus Scan Engine 38
upgrading, from Symantec CarrierScan Server 29

V

virus definitions
product name, configuring 74
updating 126
virus detection
description of technology 22
testing 25

W

Windows 2000 Server/Advanced Server
installing 31
system requirements 28
uninstalling 38

Symantec AntiVirus™ Scan Engine

CD Replacement Form

CD REPLACEMENT: After your 60-Day Limited Warranty, if your CD becomes unusable, fill out and return 1) this form, 2) your damaged CD, and 3) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement CD. *DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE.* You must be a registered customer in order to receive CD replacements.

FOR CD REPLACEMENT

Please send me: ___ CD Replacement

Name _____

Company Name _____

Street Address (No P.O. Boxes, Please) _____

City _____ State _____ Zip/Postal Code _____

Country* _____ Daytime Phone _____

Software Purchase Date _____

*This offer limited to U.S., Canada, and Mexico. Outside North America, contact your local Symantec office or distributor.

Briefly describe the problem: _____

CD Replacement Price	$ 10.00
Sales Tax (See Table)	_____
Shipping & Handling	$ 9.95
TOTAL DUE	_____

SALES TAX TABLE: AZ (5%), CA (7.25%), CO (3%), CT (6%), DC (5.75%), FL (6%), GA (4%), IA (5%), IL (6.25%), IN (5%), KS (4.9%), LA (4%), MA (5%), MD (5%), ME (6%), MI (6%), MN (6.5%), MO (4.225%), NC (6%), NJ (6%), NY (4%), OH (5%), OK (4.5%), PA (6%), SC (5%), TN (6%), TX (6.25%), VA (4.5%), WA (6.5%), WI (5%). Please add local sales tax (as well as state sales tax) in AZ, CA, FL, GA, MO, NY, OH, OK, SC, TN, TX, WA, WI.

FORM OF PAYMENT ** (CHECK ONE):

___ Check (Payable to Symantec) Amount Enclosed $ _____ __ Visa __ Mastercard __ AMEX

Credit Card Number _____ Expires _____

Name on Card (please print) _____ Signature _____

**U.S. Dollars. Payment must be made in U.S. dollars drawn on a U.S. bank.

MAIL YOUR CD REPLACEMENT ORDER TO:

Symantec Corporation
Attention: Order Processing
555 International Way
Springfield, OR 97477 (800) 441-7234
Please allow 2-3 weeks for delivery within the U.S.

Symantec and Symantec AntiVirus are trademarks of Symantec Corporation.
Other brands and products are trademarks of their respective holder/s.
© 2002 Symantec Corporation. All rights reserved. Printed in the U.S.A.

symantec™